TestOut

TestOut Security Pro – English 8.0

Objective Mappings:

TestOut Security Pro

CompTIA Security+ SY0-701

Revised: 2023-11-07

Powered by LABSIM

Contents

This document contains four objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to CompTIA SY0-701 Objective

Section	Title	Objectives
1.0	**Security Concepts**	
1.1	Security Introduction	1.1 Compare and contrast various types of security controls • 1.1.1 - Categories 1.1.1.1 - Technical 1.1.1.2 - Managerial 1.1.1.3 - Operational 1.1.1.4 - Physical 1.2 Summarize fundamental security concepts • 1.2.1 - Confidentiality, Integrity, and Availability (CIA) 2.1 Compare and contrast common threat actors and motivations • 2.1.1 - Threat actors 2.1.1.1 - Nation-state 2.1.1.5 - Organized crime
1.2	Security Controls	1.1 Compare and contrast various types of security controls • 1.1.1 - Categories 1.1.1.1 - Technical 1.1.1.2 - Managerial 1.1.1.3 - Operational 1.1.1.4 - Physical

		• 1.1.2 - Control types 1.1.2.1 - Preventive 1.1.2.2 - Deterrent 1.1.2.3 - Detective 1.1.2.4 - Corrective 1.1.2.5 - Compensating 1.1.2.6 - Directive
1.3	Use the Simulator	
2.0	**Threats, Vulnerabilities, and Mitigations**	
2.1	Understanding Attacks	2.1 Compare and contrast common threat actors and motivations • 2.1.1 - Threat actors 2.1.1.1 - Nation-state 2.1.1.2 - Unskilled attacker 2.1.1.3 - Hacktivist 2.1.1.4 - Insider threat 2.1.1.5 - Organized crime 2.1.1.6 - Shadow IT • 2.1.2 - Attributes of actors 2.1.2.1 - Internal/external 2.1.2.2 - Resources/funding 2.1.2.3 - Level of sophistication/capability • 2.1.3 - Motivations 2.1.3.1 - Data exfiltration 2.1.3.2 - Espionage

		2.1.3.3 - Service disruption 2.1.3.4 - Blackmail 2.1.3.5 - Financial gain 2.1.3.6 - Philosophical/political beliefs 2.1.3.7- Ethical 2.1.3.8 - Revenge 2.1.3.9 - Disruption/chaos 2.1.3.10 - War 2.2 Explain common threat vectors and attack surfaces • 2.2.1 - Message-based 2.2.1.1 - Email 2.2.1.2 - Short Message Service (SMS) 2.2.1.3 - Instant messaging (IM) • 2.2.2 - Image-based • 2.2.3 - File-based • 2.2.5 - Removable device • 2.2.6 - Vulnerable software 2.2.6.1 - Client-based vs. agentless • 2.2.7 - Unsupported systems and applications • 2.2.8 - Unsecure networks 2.2.8.1 - Wireless 2.2.8.2 - Wired 2.2.8.3 - Bluetooth • 2.2.9 - Open service ports • 2.2.10 - Default credentials

		• 2.2.11 - Supply chain 2.2.11.1 - Managed service providers (MSPs) 2.2.11.2 - Vendors 2.2.11.3 - Suppliers 2.3 Explain various types of vulnerabilities • 2.3.7 - Supply chain 2.3.7.1 - Service provider 2.3.7.2 - Hardware provider 2.3.7.3 - Software provider 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.4 - Application attacks 2.4.4.4 - Privilege escalation 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.8 - Least privilege 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.3 - Attack surface
2.2	Social Engineering	2.1 Compare and contrast common threat actors and motivations • 2.1.1 - Threat actors

		2.1.1.2 - Unskilled attacker 2.1.1.4 - Insider threat • 2.1.3 - Motivations 2.2 Explain common threat vectors and attack surfaces • 2.2.12 - Human vectors/social engineering 2.2.12.1 - Phishing 2.2.12.2 - Vishing 2.2.12.3 - Smishing 2.2.12.4 - Misinformation/disinformation 2.2.12.5 - Impersonation 2.2.12.6 - Business email compromise 2.2.12.7 - Pretexting 2.2.12.8 - Watering hole 2.2.12.9 - Brand impersonation 2.2.12.10 - Typosquatting 5.6 Given a scenario, implement security awareness practices • 5.6.3 - User guidance and training 5.6.3.6 - Social engineering • 5.6.5 - Development
2.3	Malware	2.4 Given a scenario, analyze indicators of malicious activity • 2.4.1 - Malware attacks 2.4.1.1 - Ransomware 2.4.1.2 - Trojan 2.4.1.3 - Worm 2.4.1.4 - Spyware

		2.4.1.5 - Bloatware 2.4.1.6 - Virus 2.4.1.7 - Keylogger 2.4.1.8 - Logic bomb 2.4.1.9 - Rootkit
3.0	**Cryptographic Solutions**	
3.1	Cryptography	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.1 - Public key infrastructure (PKI) 1.4.1.1 - Public key 1.4.1.2 - Private key 1.4.1.3 - Key escrow • 1.4.2 - Encryption 1.4.2.3 - Asymmetric 1.4.2.4 - Symmetric 1.4.2.6 - Algorithms 1.4.2.7 - Key length • 1.4.4 - Obfuscation 1.4.4.1 - Steganography • 1.4.5 - Hashing • 1.4.6 - Salting • 1.4.7 - Digital signatures • 1.4.9 - Blockchain

		2.4 Given a scenario, analyze indicators of malicious activity • 2.4.5 - Cryptographic attacks 2.4.5.1 - Downgrade 2.4.5.2 - Collision 2.4.5.3 - Birthday
3.2	Cryptography Implementations	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.2 - Encryption 1.4.2.1.1 - Full-disk 1.4.2.3 - Asymmetric 1.4.2.4 - Symmetric 1.4.2.5 - Key exchange • 1.4.3 - Tools 1.4.3.1 - Trusted Platform Module (TPM) 1.4.3.2 - Hardware security module (HSM) 1.4.3.3 - Key management system 1.4.3.4 - Secure enclave • 1.4.4 - Obfuscation 1.4.4.1 - Steganography • 1.4.5 - Hashing • 1.4.7 - Digital signatures
3.3	Hashing	1.4 Explain the importance of using appropriate cryptographic solutions

		• 1.4.2 - Encryption 1.4.2.6 - Algorithms • 1.4.5 - Hashing • 1.4.6 - Salting • 1.4.7 - Digital signatures
3.4	Encryption	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.2 - Encryption 1.4.2.1.1 - Full-disk 1.4.2.1.3 - File 1.4.2.1.5 - Database • 1.4.3 - Tools 1.4.3.1 - Trusted Platform Module (TPM) 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.6 - Encryption
3.5	Public Key Infrastructure	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.1 - Public key infrastructure (PKI) 1.4.1.1 - Public key 1.4.1.2 - Private key 1.4.1.3 - Key escrow • 1.4.7 - Digital signatures

		• 1.4.11 - Certificates 1.4.11.1 - Certificate authorities 1.4.11.2 - Certificate revocation lists (CRLs) 1.4.11.3 - Online Certificate Status Protocol (OCSP) 1.4.11.4 - Self-signed 1.4.11.5 - Third-party 1.4.11.6 - Root of trust 1.4.11.7 - Certificate signing request (CSR) generation 1.4.11.8 - Wildcard 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.6 - Application security 4.1.6.1 - Input validation 4.1.6.2 - Secure cookies 4.1.6.3 - Static code analysis 4.1.6.4 - Code signing
4.0	**Identity and Access Management**	
4.1	Access Control Models	1.2 Summarize fundamental security concepts • 1.2.1 - Confidentiality, Integrity, and Availability (CIA) • 1.2.2 - Non-repudiation • 1.2.3 - Authentication, Authorization, and Accounting (AAA) 1.2.3.1 - Authenticating people 1.2.3.2 - Authenticating systems 1.2.3.3 - Authorization models • 1.2.4 - Gap analysis

		• 1.2.5 - Zero trust 1.2.5.1 - Control plane 1.2.5.1.1 - Adaptive identity 1.2.5.1.2 - Threat scope reduction 1.2.5.1.3 - Policy-driven access control 1.2.5.1.4 - Policy Administrator 1.2.5.1.5 - Policy Engine 1.2.5.2 - Data plane 1.2.5.2.1 - Implicit trust zones 1.2.5.2.2 - Subject/System 1.2.5.2.3 - Policy enforcement point 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.2 - Access control • 2.5.8 - Least privilege 4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts • 4.6.2 - Permission assignments and implications • 4.6.3 - Identity proofing • 4.6.8 - Access controls 4.6.8.1 - Mandatory 4.6.8.2 - Discretionary 4.6.8.3 - Role-based 4.6.8.4 - Rule-based 4.6.8.5 - Attribute-based 4.6.8.6 - Time-of-day restrictions 4.6.8.7 - Least privilege • 4.6.9 - Multifactor authentication

		4.6.9.1.2 - Hard/soft authentication tokens 4.6.9.2 - Factors 4.6.9.2.1 - Something you know 4.6.9.2.2 - Something you have 4.6.9.2.3 - Something you are 4.6.9.2.4 - Somewhere you are 5.1 Summarize elements of effective security governance • 5.1.2 - Policies 5.1.2.2 - Information security policies
4.2	Authentication	1.2 Summarize fundamental security concepts • 1.2.3 - Authentication, Authorization, and Accounting (AAA) 1.2.3.1 - Authenticating people 1.2.3.2 - Authenticating systems 1.2.3.3 - Authorization models 4.6 Given a scenario, implement and maintain identity and access management • 4.6.4 - Federation • 4.6.5 - Single sign-on (SSO) 4.6.5.1 - Lightweight Directory Access Protocol (LDAP) 4.6.5.2 - Open authorization (OAuth) 4.6.5.3 - Security Assertions Markup Language (SAML) • 4.6.6 - Interoperability • 4.6.7 - Attestation

		• 4.6.9 - Multifactor authentication 4.6.9.1 - Implementations 4.6.9.1.1 - Biometrics 4.6.9.1.2 - Hard/soft authentication tokens 4.6.9.1.3 - Security keys 4.6.9.2 - Factors 4.6.9.2.1 - Something you know 4.6.9.2.2 - Something you have 4.6.9.2.3 - Something you are 4.6.9.2.4 - Somewhere you are
4.3	Authorization	1.2 Summarize fundamental security concepts • 1.2.3 - Authentication, Authorization, and Accounting (AAA) 1.2.3.3 - Authorization models 1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.4 - Obfuscation 1.4.4.2 - Tokenization 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.2 - Access control 2.5.2.1 - Access control list (ACL) 2.5.2.2 - Permissions 4.6 Given a scenario, implement and maintain identity and access management • 4.6.2 - Permission assignments and implications

		• 4.6.5 - Single sign-on (SSO) • 4.6.8 - Access controls 4.6.8.2 - Discretionary
4.4	Active Directory Overview	1.2 Summarize fundamental security concepts • 1.2.3 - Authentication, Authorization, and Accounting (AAA) 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.4 - Operating system security 4.5.4.1 - Group Policy
4.5	Hardening Authentication	1.2 Summarize fundamental security concepts • 1.2.3 - Authentication, Authorization, and Accounting (AAA) 1.2.3.1 - Authenticating people 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.7 - Indicators 2.4.7.1 - Account lockout 2.4.7.2 - Concurrent session usage 2.4.7.3 - Blocked content 2.4.7.4 - Impossible travel 2.4.7.6 - Resource inaccessibility 4.5 Given a scenario, modify enterprise capabilities to enhance security

		• 4.5.4 - Operating system security 4.5.4.1 - Group Policy 4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts • 4.6.2 - Permission assignments and implications • 4.6.9 - Multifactor authentication 4.6.9.1.3 - Security keys 4.6.9.2.2 - Something you have • 4.6.10 - Password concepts 4.6.10.1 - Password best practices 4.6.10.1.1 - Length 4.6.10.1.2 - Complexity 4.6.10.1.3 - Reuse 4.6.10.1.4 - Expiration 4.6.10.1.5 - Age 4.6.10.2 - Password managers 4.6.10.3 - Passwordless • 4.6.11 - Privileged access management tools 4.6.11.1 - Just-in-time permissions 4.6.11.2 - Password vaulting 4.6.11.3 - Temporal accounts
4.6	Linux Users	2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.11 - Hardening techniques

		2.5.11.6 - Default password changes 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.6 - Application security 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.4 - Operating system security 4.5.4.2 - SELinux 4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts • 4.6.10 - Password concepts 4.6.10.1.3 - Reuse 4.6.10.1.4 - Expiration
4.7	Linux Groups	4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts
4.8	Remote Access	3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.1 - Virtual private network (VPN) 3.2.2.2 - Remote access 3.2.2.3 - Tunneling 3.2.2.3.2 - Internet protocol security (IPSec)

		4.1 Given a scenario, apply common security techniques to computing resources • 4.1.5 - Wireless security settings 4.1.5.2 - AAA/Remote Authentication Dial-In User Service (RADIUS)
4.9	Network Authentication	4.6 Given a scenario, implement and maintain identity and access management • 4.6.4 - Federation • 4.6.5 - Single sign-on (SSO) 4.6.5.1 - Lightweight Directory Access Protocol (LDAP) 4.6.5.2 - Open authorization (OAuth) 4.6.5.3 - Security Assertions Markup Language (SAML)
5.0	**Network Architecture**	
5.1	Enterprise Network Architecture	3.1 Compare and contrast security implications of different architecture models • 3.1.1 - Architecture and infrastructure concepts 3.1.1.1 - Cloud 3.1.1.1.1 - Responsibility matrix 3.1.1.1.2 - Hybrid considerations 3.1.1.1.3 - Third-party vendors 3.1.1.2 - Infrastructure as code (IaC) 3.1.1.3 - Serverless 3.1.1.4 - Microservices 3.1.1.5 - Network infrastructure 3.1.1.5.1 - Physical isolation 3.1.1.5.1.1 - Air-gapped 3.1.1.5.2 - Logical segmentation 3.1.1.5.3 - Software-defined networking (SDN) 3.1.1.6 - On-premises

		3.1.1.7 - Centralized/decentralized • 3.1.2 - Considerations 3.1.2.1 - Availability 3.1.2.2 - Resilience 3.1.2.3 - Cost 3.1.2.4 - Responsiveness 3.1.2.5 - Scalability 3.1.2.6 - Ease of deployment 3.1.2.7 - Risk transference 3.1.2.8 - Ease of recovery 3.1.2.9 - Patch availability 3.1.2.10 - Inability to patch 3.1.2.11 - Power 3.1.2.12 - Compute 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.1 - Device placement 3.2.1.2 - Security zones 3.2.1.3 - Attack surface 3.2.1.4 - Connectivity 3.2.1.5 - Failure modes 3.2.1.5.1 - Fail-open 3.2.1.5.2 - Fail-closed 3.2.1.6 - Device attribute 3.2.1.6.1 - Active vs. passive 3.2.1.6.2 - Inline vs. tap/monitor 3.2.1.7.4 - Load balancer • 3.2.3 - Selection of effective controls
5.2	Security Appliances	1.2 Summarize fundamental security concepts

		• 1.2.7 - Deception and disruption technology 1.2.7.1 - Honeypot 1.2.7.2 - Honeynet 1.2.7.3 - Honeyfile 1.2.7.4 - Honeytoken 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.2 - Security zones 3.2.1.5 - Failure modes 3.2.1.5.1 - Fail-open 3.2.1.5.2 - Fail-closed 3.2.1.7 - Network appliances 3.2.1.7.1 - Jump server 3.2.1.7.2 - Proxy server 3.2.1.7.3 - Intrusion prevention system (IPS)/intrusion detection system (IDS) 3.2.1.7.4 - Load balancer 3.2.1.7.5 - Sensors 3.2.1.9.2 - Unified threat management (UTM) 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.1 - Firewall 4.5.1.4 - Screened subnets • 4.5.2 - IDS/IPS 4.5.2.1 - Trends 4.5.2.2 - Signatures • 4.5.3 - Web filter

		4.5.3.1 - Agent-based 4.5.3.2 - Centralized proxy 4.5.3.3 - Universal Resource Locator (URL) scanning 4.5.3.4 - Content categorization 4.5.3.5 - Block rules 4.5.3.6 - Reputation • 4.5.6 - DNS filtering
5.3	Screened Subnets	3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.1 - Virtual private network (VPN) 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.1 - Firewall 4.5.1.4 - Screened subnets
5.4	Firewalls	2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.11 - Hardening techniques 2.5.11.3 - Host-based firewall 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.9 - Firewall types 3.2.1.9.1 - Web application firewall (WAF) 3.2.1.9.2 - Unified threat management (UTM)

		3.2.1.9.3 - Next-generation firewall (NGFW) 3.2.1.9.4 - Layer 4/Layer 7 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.1 - Firewall 4.5.1.1 - Rules 4.5.1.2 - Access lists 4.5.1.3 - Ports/protocols 4.5.1.4 - Screened subnets
5.5	Virtual Private Networks	3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.1 - Virtual private network (VPN) 3.2.2.2 - Remote access 3.2.2.3 - Tunneling 3.2.2.3.1 - Transport Layer Security (TLS) 3.2.2.3.2 - Internet protocol security (IPSec) 3.2.2.4 - Software-defined wide area network (SD-WAN) 3.2.2.5 - Secure access service edge (SASE)
5.6	Network Access Control	4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.10. Network access control (NAC)
5.7	Network Device Vulnerabilities	2.3 Explain various types of vulnerabilities • 2.3.9 - Misconfiguration • 2.3.11 - Zero-day

		2.4 Given a scenario, analyze indicators of malicious activity • 2.4.4 - Application attacks 2.4.4.4 - Privilege escalation 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.1 - Segmentation • 2.5.11 - Hardening techniques 2.5.11.6 - Default password changes 4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts • 4.6.10 - Password concepts 4.6.10.1 - Password best practices 4.6.10.1.1 - Length 4.6.10.1.2 - Complexity 4.6.10.1.3 - Reuse 4.6.10.1.4 - Expiration 4.6.10.1.5 - Age 5.1 Summarize elements of effective security governance • 5.1.3 - Standards 5.1.3.1 - Password
5.8	Network Applications	1.4 Explain the importance of using appropriate cryptographic solutions

		• 1.4.7 - Digital signatures 4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.1 - Vulnerability scan 4.3.1.2 - Application security 4.3.1.2.1 - Static analysis 4.3.1.2.2 - Dynamic analysis 4.3.1.2.3 - Package monitoring • 4.3.3 - Vulnerability response and remediation 4.3.3.1 - Patching
5.9	Switch Security and Attacks	3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.8 - Port security 3.2.1.8.1 - 802.1X 3.2.1.8.2 - Extensible Authentication Protocol (EAP) 3.3 Compare and contrast concepts and strategies to protect data • 3.3.4 - Methods to secure data 3.3.4.7 - Segmentation 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.2 - Hardening targets

		4.1.2.3 - Switches • 4.1.5 - Wireless security settings 4.1.5.2 - AAA/Remote Authentication Dial-In User Service (RADIUS) 4.1.5.4 - Authentication protocols 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.5 - Implementation of secure protocols
5.10	Router Security	1.1 Compare and contrast various types of security controls • 1.1.1 - Categories 1.1.1.4 - Physical 2.2 Explain common threat vectors and attack surfaces • 2.2.10 - Default credentials 2.3 Explain various types of vulnerabilities • 2.3.4 - Hardware 2.3.4.1 - Firmware 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.2 - Access control 2.5.2.1 - Access control list (ACL) 2.5.2.2 - Permissions

		• 2.5.11 - Hardening techniques 2.5.11.5 - Disabling ports/protocols 2.5.11.6 - Default password changes 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.2 - Remote access 3.3 Compare and contrast concepts and strategies to protect data • 3.3.4 - Methods to secure data 3.3.4.7 - Segmentation 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.2 - Hardening targets 4.1.2.4 - Routers 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.5 - Implementation of secure protocols 4.5.5.1 - Protocol selection 5.1 Summarize elements of effective security governance • 5.1.3 - Standards 5.1.3.2 - Access control

6.0	Resiliency and Site Security	
6.1	Physical Threats	1.2 Summarize fundamental security concepts • 1.2.6 - Physical security 1.2.6.1 - Bollards 1.2.6.2 - Access control vestibule 1.2.6.3 - Fencing 1.2.6.4 - Video surveillance 1.2.6.5 - Security guard 1.2.6.6 - Access badge 1.2.6.7 - Lighting 1.2.6.8 - Sensors 1.2.6.8.1 - Infrared 1.2.6.8.2 - Pressure 1.2.6.8.3 - Microwave 1.2.6.8.4 - Ultrasonic 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.2 - Physical attacks 2.4.2.1 - Brute force 2.4.2.2 - Radio frequency identification (RFID) cloning 2.4.2.3 - Environmental 3.4 Explain the importance of resilience and recovery in security architecture • 3.4.9 - Power 4.6 Given a scenario, implement and maintain identity and access management • 4.6.9 - Multifactor authentication

		4.6.9.1.1 - Biometrics
6.2	Monitoring and Reconnaissance	2.2 Explain common threat vectors and attack surfaces • 2.2.8 - Unsecure networks • 2.2.9 - Open service ports 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.7 - Monitoring 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.8. Monitoring 4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.3.1 - Open-source intelligence (OSINT) 4.4 Explain security alerting and monitoring concepts and tools • 4.4.1 - Monitoring computing resources 4.4.1.1 - Systems 4.4.1.3 - Infrastructure • 4.4.3 - Tools 4.4.3.6 - Vulnerability scanners

		4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.1 - Firewall 4.5.1.3 - Ports/protocols 4.9 Given a scenario, use data sources to support an investigation • 4.9.2 - Data sources 4.9.2.4 - Packet captures 5.4 Summarize elements of effective security compliance • 5.4.3 - Compliance monitoring 5.5 Explain types and purposes of audits and assessments • 5.5.2 - Internal 5.5.2.1 - Compliance • 5.5.4 - Penetration testing 5.5.4.8 - Reconnaissance 5.5.4.8.1 - Passive 5.5.4.8.2 - Active
6.3	Intrusion Detection	2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.11 - Hardening techniques 2.5.11.4 - Host-based intrusion prevention system (HIPS)

		3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.6.2 - Inline vs. tap/monitor 3.2.1.7.3 - Intrusion prevention system (IPS)/intrusion detection system (IDS) 3.2.1.7.5 - Sensors 4.3 Explain various activities associated with vulnerability management • 4.3.2 - Analysis 4.3.2.1 - Confirmation 4.3.2.1.1 - False positive 4.3.2.1.2 - False negative 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.2 - IDS/IPS 4.5.2.1 - Trends 4.5.2.2 - Signatures • 4.5.12. User behavior analytics 5.6 Given a scenario, implement security awareness practices • 5.6.2 - Anomalous behavior recognition 5.6.2.2 - Unexpected
6.4	Protocol Analyzers	2.4 Given a scenario, analyze indicators of malicious activity

		• 2.4.3 - Network attacks 2.4.3.4 - On-path 2.4.3.5 - Credential replay 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.11 - Hardening techniques 2.5.11.5 - Disabling ports/protocols 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.8. Monitoring 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.1 - Firewall 4.5.1.3 - Ports/protocols • 4.5.5 - Implementation of secure protocols 4.9 Given a scenario, use data sources to support an investigation • 4.9.2 - Data sources 4.9.2.4 - Packet captures
6.5	Analyzing Network Attacks	2.1 Compare and contrast common threat actors and motivations • 2.1.3 - Motivations

		2.1.3.1 - Data exfiltration 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.3 - Network attacks 2.4.3.1 - Distributed denial-of-service (DDoS) 2.4.3.1.1 - Amplified 2.4.3.1.2 - Reflected 2.4.3.2 - Domain Name System (DNS) attacks 2.4.3.3 - Wireless 2.4.3.4 - On-path 2.4.3.5 - Credential replay 2.4.3.6 - Malicious code • 2.4.4 - Application attacks 2.4.4.4 - Privilege escalation 4.7 Explain the importance of automation and orchestration related to secure operations • 4.7.1 - Use cases of automation and scripting 4.9 Given a scenario, use data sources to support an investigation • 4.9.2 - Data sources 4.9.2.4 - Packet captures 5.5 Explain types and purposes of audits and assessments • 5.5.4 - Penetration testing 5.5.4.8 - Reconnaissance

6.6	Analyzing Password Attacks	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.5 - Hashing • 1.4.6 - Salting 2.2 Explain common threat vectors and attack surfaces • 2.2.10 - Default credentials • 2.2.12 - Human vectors/social engineering 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.6 - Password attacks 2.4.6.1 - Spraying 2.4.6.2 - Brute force 5.6 Given a scenario, implement security awareness practices • 5.6.3 - User guidance and training 5.6.3.4 - Password management
7.0	**Vulnerability Management**	
7.1	Vulnerability Management	1.1 Compare and contrast various types of security controls • 1.1.2 - Control types 1.1.2.5 - Compensating

2.3 Explain various types of vulnerabilities

- 2.3.2 - Operating system (OS)-based
- 2.3.4 - Hardware

    2.3.4.1 - Firmware
    2.3.4.2 - End-of-life
    2.3.4.3 - Legacy

4.3 Explain various activities associated with vulnerability management

- 4.3.1 - Identification methods

    4.3.1.1 - Vulnerability scan
    4.3.1.3 - Threat feed
    4.3.1.3.1 - Open-source intelligence (OSINT)
    4.3.1.3.2 - Proprietary/third-party
    4.3.1.3.3 - Information-sharing organization
    4.3.1.3.4 - Dark web
    4.3.1.4 - Penetration testing
    4.3.1.5 - Responsible disclosure program
    4.3.1.5.1 - Bug bounty program
    4.3.1.6 - System/process audit

- 4.3.2 - Analysis

    4.3.2.1 - Confirmation
    4.3.2.2 - Prioritize
    4.3.2.3 - Common Vulnerability Scoring System (CVSS)
    4.3.2.4 - Common Vulnerability Enumeration (CVE)
    4.3.2.5 - Vulnerability classification
    4.3.2.6 - Exposure factor
    4.3.2.7 - Environmental variables
    4.3.2.8 - Industry/organizational impact
    4.3.2.9 - Risk tolerance

		• 4.3.3 - Vulnerability response and remediation 4.3.3.1 - Patching 4.3.3.2 - Insurance 4.3.3.3 - Segmentation 4.3.3.4 - Compensating controls 4.3.3.5 - Exceptions and exemptions • 4.3.4 - Validation of remediation 4.3.4.1 - Rescanning 4.3.4.2 - Audit 4.3.4.3 - Verification 4.4 Explain security alerting and monitoring concepts and tools • 4.4.3 - Tools 4.4.3.6 - Vulnerability scanners 4.8 Explain appropriate incident response activities • 4.8.5 - Threat hunting 4.9 Given a scenario, use data sources to support an investigation • 4.9.2 - Data sources 4.9.2.1 - Vulnerability scans
7.2	Vulnerability Scanning	2.2 Explain common threat vectors and attack surfaces • 2.2.6 - Vulnerable software

		4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.1 - Vulnerability scan 4.3.1.2 - Application security 4.3.1.2.1 - Static analysis 4.3.1.2.2 - Dynamic analysis 4.3.1.2.3 - Package monitoring • 4.3.2 - Analysis 4.3.2.4 - Common Vulnerability Enumeration (CVE) 4.3.2.5 - Vulnerability classification 4.4 Explain security alerting and monitoring concepts and tools • 4.4.1 - Monitoring computing resources 4.4.1.1 - Systems 4.4.1.2 - Applications 4.4.1.3 - Infrastructure • 4.4.2 - Activities 4.4.2.3 - Scanning 4.4.2.4 - Reporting • 4.4.3 - Tools 4.4.3.6 - Vulnerability scanners 4.9 Given a scenario, use data sources to support an investigation

		• 4.9.2 - Data sources 4.9.2.3 - Dashboards
7.3	Alerting and Monitoring	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.4 - Obfuscation 1.4.4.2 - Tokenization 1.4.4.3 - Data masking 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.7 - Monitoring 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.7.5 - Sensors 3.3 Compare and contrast concepts and strategies to protect data • 3.3.3 - General data considerations 3.3.3.1.1 - Data at rest 3.3.3.1.2 - Data in transit 3.3.3.1.3 - Data in use • 3.3.4 - Methods to secure data 3.3.4.2 - Encryption 3.3.4.4 - Masking 3.3.4.5 - Tokenization

		3.3.4.8 - Permission restrictions 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.8. Monitoring 4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.1 - Vulnerability scan 4.4 Explain security alerting and monitoring concepts and tools • 4.4.1 - Monitoring computing resources 4.4.1.1 - Systems 4.4.1.3 - Infrastructure • 4.4.2 - Activities 4.4.2.1 - Log aggregation 4.4.2.2 - Alerting 4.4.2.4 - Reporting 4.4.2.5 - Archiving 4.4.2.6 - Alert response and remediation/validation 4.4.2.6.2 - Alert tuning • 4.4.3 - Tools 4.4.3.1 - Security Content Automation Protocol (SCAP) 4.4.3.2 - Benchmarks 4.4.3.3 - Agents/agentless 4.4.3.3.1 - Security information and event management (SIEM) 4.4.3.3.2 - Antivirus 4.4.3.3.3 - Data loss prevention (DLP)

		4.4.3.4 - Simple Network Management Protocol (SNMP) traps 4.4.3.5 - NetFlow 4.4.3.6 - Vulnerability scanners 4.9 Given a scenario, use data sources to support an investigation • 4.9.1 - Log data 4.9.1.1 - Firewall logs 4.9.1.3 - Endpoint logs 4.9.1.4 - OS-specific security logs 4.9.1.5 - IPS/IDS logs 4.9.1.6 - Network logs • 4.9.2 - Data sources 4.9.2.3 - Dashboards 5.1 Summarize elements of effective security governance • 5.1.4 - Procedures 5.1.4.3 - Playbooks 5.6 Given a scenario, implement security awareness practices • 5.6.4 - Reporting and monitoring
7.4	Penetration Testing	2.2 Explain common threat vectors and attack surfaces • 2.2.12 - Human vectors/social engineering 4.3 Explain various activities associated with vulnerability management

		• 4.3.1 - Identification methods 4.3.1.3.1 - Open-source intelligence (OSINT) 4.3.1.4 - Penetration testing 4.3.1.5.1 - Bug bounty program 4.4 Explain security alerting and monitoring concepts and tools • 4.4.3 - Tools 4.4.3.6 - Vulnerability scanners 5.3 Explain the processes associated with third-party risk assessment and management • 5.3.3 - Agreement types 5.3.3.5 - Work order (WO)/statement of work (SOW) • 5.3.6 - Rules of engagement 5.5 Explain types and purposes of audits and assessments • 5.5.4 - Penetration testing 5.5.4.1 - Physical 5.5.4.2 - Offensive 5.5.4.3 - Defensive 5.5.4.4 - Integrated 5.5.4.5 - Known environment 5.5.4.6 - Partially known environment 5.5.4.7 - Unknown environment 5.5.4.8 - Reconnaissance 5.5.4.8.1 - Passive 5.5.4.8.2 - Active

8.0	Network and Endpoint Security	
8.1	Operating System Hardening	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.2 - Encryption 1.4.2.1.1 - Full-disk 2.2 Explain common threat vectors and attack surfaces • 2.2.5 - Removable device 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.2 - Access control • 2.5.3 - Application allow list • 2.5.5 - Patching • 2.5.6 - Encryption • 2.5.7 - Monitoring • 2.5.8 - Least privilege • 2.5.9 - Configuration enforcement • 2.5.10 - Decommissioning • 2.5.11 - Hardening techniques 2.5.11.2 - Installation of endpoint protection 2.5.11.3 - Host-based firewall 2.5.11.5 - Disabling ports/protocols 2.5.11.6 - Default password changes 2.5.11.7 - Removal of unnecessary software

		4.1 Given a scenario, apply common security techniques to computing resources • 4.1.1 - Secure baselines 4.1.1.1 - Establish 4.1.1.2 - Deploy 4.1.1.3 - Maintain • 4.1.2 - Hardening targets 4.1.2.2 - Workstations 4.3 Explain various activities associated with vulnerability management • 4.3.3 - Vulnerability response and remediation 4.3.3.1 - Patching 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.4 - Operating system security 4.5.4.1 - Group Policy 4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts • 4.6.8 - Access controls 4.6.8.7 - Least privilege • 4.6.9 - Multifactor authentication

		4.7 Explain the importance of automation and orchestration related to secure operations • 4.7.1 - Use cases of automation and scripting 4.7.1.4 - Security groups
8.2	File Server Security	1.2 Summarize fundamental security concepts • 1.2.6 - Physical security 1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.2 - Encryption 1.4.2.1.1 - Full-disk 1.4.2.1.3 - File 2.2 Explain common threat vectors and attack surfaces • 2.2.3 - File-based 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.2 - Access control 2.5.2.1 - Access control list (ACL) 2.5.2.2 - Permissions • 2.5.8 - Least privilege • 2.5.11 - Hardening techniques 2.5.11.7 - Removal of unnecessary software

		3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.1 - Virtual private network (VPN) 3.2.2.3.2 - Internet protocol security (IPSec) 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.2 - Hardening targets 4.1.2.6 - Servers 4.2 Explain the security implications of proper hardware, software, and data asset management • 4.2.1 - Acquisition/procurement process 4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.6 - System/process audit 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.5 - Implementation of secure protocols • 4.5.8. File integrity monitoring 4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts • 4.6.8 - Access controls

		4.6.8.7 - Least privilege
8.3	Linux Host Security	2.2 Explain common threat vectors and attack surfaces • 2.2.5 - Removable device 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.5 - Patching • 2.5.11 - Hardening techniques 2.5.11.3 - Host-based firewall 2.5.11.4 - Host-based intrusion prevention system (HIPS) 2.5.11.5 - Disabling ports/protocols 2.5.11.7 - Removal of unnecessary software
8.4	Wireless Overview	4.1 Given a scenario, apply common security techniques to computing resources • 4.1.3. Wireless devices 4.1.3.1 - Installation considerations 4.1.3.1.1 - Site surveys 4.1.3.1.2 - Heat maps • 4.1.5 - Wireless security settings 4.1.5.1 - Wi-Fi Protected Access 3 (WPA3) 4.1.5.2 - AAA/Remote Authentication Dial-In User Service (RADIUS)
8.5	Wireless Attacks	2.2 Explain common threat vectors and attack surfaces • 2.2.8 - Unsecure networks

		2.2.8.1 - Wireless 2.2.8.3 - Bluetooth 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.2 - Physical attacks 2.4.2.2 - Radio frequency identification (RFID) cloning • 2.4.3 - Network attacks 2.4.3.3 - Wireless 2.4.3.5 - Credential replay 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.3. Wireless devices 4.1.3.1 - Installation considerations • 4.1.5 - Wireless security settings 4.1.5.1 - Wi-Fi Protected Access 3 (WPA3) 4.1.5.4 - Authentication protocols
8.6	Wireless Defenses	2.2 Explain common threat vectors and attack surfaces • 2.2.8 - Unsecure networks 2.2.8.1 - Wireless • 2.2.10 - Default credentials

		2.3 Explain various types of vulnerabilities • 2.3.4 - Hardware 2.3.4.1 - Firmware 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.11 - Hardening techniques 2.5.11.6 - Default password changes 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.7.3 - Intrusion prevention system (IPS)/intrusion detection system (IDS) 3.2.1.8 - Port security 3.2.1.8.1 - 802.1X 3.2.1.8.2 - Extensible Authentication Protocol (EAP) • 3.2.2 - Secure communication/access 3.2.2.3.1 - Transport Layer Security (TLS) 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.3. Wireless devices 4.1.3.1 - Installation considerations • 4.1.5 - Wireless security settings

		4.1.5.1 - Wi-Fi Protected Access 3 (WPA3) 4.1.5.2 - AAA/Remote Authentication Dial-In User Service (RADIUS) 4.1.5.3 - Cryptographic protocols 4.1.5.4 - Authentication protocols
8.7	Data Transmission Security	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.2 - Encryption 1.4.2.2 - Transport/communication 1.4.2.3 - Asymmetric 1.4.2.5 - Key exchange • 1.4.11 - Certificates 1.4.11.1 - Certificate authorities 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.3 - Network attacks 2.4.3.2 - Domain Name System (DNS) attacks 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.1 - Virtual private network (VPN) 3.2.2.2 - Remote access 3.2.2.3 - Tunneling 3.2.2.3.1 - Transport Layer Security (TLS) 3.2.2.3.2 - Internet protocol security (IPSec)

8.8	Web Application Security	2.3 Explain various types of vulnerabilities • 2.3.1 - Application 2.3.1.1 - Memory injection 2.3.1.2 - Buffer overflow 2.3.1.3 - Race conditions 2.3.1.3.1 - Time-of-check (TOC) 2.3.1.3.2 - Time-of-use (TOU) 2.3.1.4 - Malicious update • 2.3.3 - Web-based 2.3.3.1 - Structured Query Language injection (SQLi) 2.3.3.2 - Cross-site scripting (XSS) • 2.3.4 - Hardware • 2.3.11 - Zero-day 2.4 Given a scenario, analyze indicators of malicious activity • 2.4.3 - Network attacks 2.4.3.5 - Credential replay • 2.4.4 - Application attacks 2.4.4.1 - Injection 2.4.4.2 - Buffer overflow 2.4.4.3 - Replay 2.4.4.4 - Privilege escalation 2.4.4.5 - Forgery 2.4.4.6 - Directory traversal 2.5 Explain the purpose of mitigation techniques used to secure the enterprise

		• 2.5.5 - Patching 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.7.3 - Intrusion prevention system (IPS)/intrusion detection system (IDS) 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.6 - Application security 4.1.6.2 - Secure cookies 4.6 Given a scenario, implement and maintain identity and access management • 4.6.5 - Single sign-on (SSO) 4.6.5.1 - Lightweight Directory Access Protocol (LDAP)
8.9	Application Development and Security	1.3 Explain the importance of change management processes and the impact to security • 1.3.4 -Version control 2.2 Explain common threat vectors and attack surfaces • 2.2.7 - Unsupported systems and applications 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.2 - Access control

		2.5.2.2 - Permissions • 2.5.3 - Application allow list • 2.5.5 - Patching • 2.5.7 - Monitoring • 2.5.11 - Hardening techniques 2.5.11.2 - Installation of endpoint protection 2.5.11.3 - Host-based firewall 2.5.11.7 - Removal of unnecessary software 3.3 Compare and contrast concepts and strategies to protect data • 3.3.4 - Methods to secure data 3.3.4.6 - Obfuscation 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.1 - Secure baselines 4.1.1.1 - Establish • 4.1.6 - Application security 4.1.6.1 - Input validation 4.1.6.2 - Secure cookies 4.1.6.3 - Static code analysis 4.1.6.4 - Code signing • 4.1.7. Sandboxing

		4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.2 - Application security 4.3.1.2.1 - Static analysis 4.3.1.2.2 - Dynamic analysis 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.4 - Operating system security 4.5.4.2 - SELinux 4.6 Given a scenario, implement and maintain identity and access management • 4.6.1 - Provisioning/de-provisioning user accounts • 4.6.8 - Access controls 4.6.8.7 - Least privilege 4.7 Explain the importance of automation and orchestration related to secure operations • 4.7.1 - Use cases of automation and scripting 4.7.1.1 - User provisioning 4.7.1.2 - Resource provisioning 4.7.1.4 - Security groups 4.7.1.5 - Ticket creation 4.7.1.7 - Enabling/disabling services and access 4.7.1.9 - Integrations and Application programming interfaces (APIs) • 4.7.2 - Benefits

		4.7.2.1 - Efficiency/time saving 4.7.2.2 - Enforcing baselines 4.7.2.5 - Staff retention • 4.7.3 - Other considerations 4.7.3.1 - Complexity 4.7.3.2 - Cost 4.7.3.3 - Single point of failure 4.7.3.4 - Technical debt 4.7.3.5 - Ongoing supportability 5.1 Summarize elements of effective security governance • 5.1.2 - Policies 5.1.2.6 - Software development lifecycle (SDLC) 5.2 Explain elements of the risk management process • 5.2.3 - Risk analysis 5.2.3.8 - Exposure factor
9.0	**Incident Response**	
9.1	Incident Response and Mitigation	2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.1 - Segmentation • 2.5.4 - Isolation 4.8 Explain appropriate incident response activities

		• 4.8.1 - Process 4.8.1.1 - Preparation 4.8.1.2 - Detection 4.8.1.3 - Analysis 4.8.1.4 - Containment 4.8.1.5 - Eradication 4.8.1.6 - Recovery 4.8.1.7 - Lessons learned 5.1 Summarize elements of effective security governance • 5.1.4 - Procedures 5.1.4.3 - Playbooks
9.2	Log Management	2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.7 - Monitoring 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.7.3 - Intrusion prevention system (IPS)/intrusion detection system (IDS) 3.2.1.7.5 - Sensors 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.1 - Secure baselines 4.1.1.1 - Establish

		4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.1 - Vulnerability scan • 4.3.2 - Analysis 4.3.2.4 - Common Vulnerability Enumeration (CVE) 4.4 Explain security alerting and monitoring concepts and tools • 4.4.2 - Activities 4.4.2.1 - Log aggregation 4.4.2.2 - Alerting • 4.4.3 - Tools 4.4.3.3.1 - Security information and event management (SIEM) 4.4.3.5 - NetFlow 4.4.3.6 - Vulnerability scanners 4.9 Given a scenario, use data sources to support an investigation • 4.9.1 - Log data 4.9.1.1 - Firewall logs 4.9.1.2 - Application logs 4.9.1.3 - Endpoint logs 4.9.1.4 - OS-specific security logs 4.9.1.5 - IPS/IDS logs 4.9.1.6 - Network logs 4.9.1.7 - Metadata

		• 4.9.2 - Data sources 4.9.2.3 - Dashboards 4.9.2.4 - Packet captures
9.3	Digital Forensics	4.8 Explain appropriate incident response activities • 4.8.6 - Digital forensics 4.8.6.1 - Legal hold 4.8.6.2 - Chain of custody 4.8.6.3 - Acquisition 4.8.6.4 - Reporting 4.8.6.5 - Preservation 4.8.6.6 - E-discovery 4.9 Given a scenario, use data sources to support an investigation • 4.9.2 - Data sources 4.9.2.1 - Vulnerability scans 4.9.2.3 - Dashboards 4.9.2.4 - Packet captures
9.4	Redundancy	3.1 Compare and contrast security implications of different architecture models • 3.1.1 - Architecture and infrastructure concepts 3.1.1.1.3 - Third-party vendors 3.1.1.5 - Network infrastructure 3.1.1.14 - High availability • 3.1.2 - Considerations

		3.1.2.11 - Power 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.6.1 - Active vs. passive 3.2.1.7.4 - Load balancer 3.4 Explain the importance of resilience and recovery in security architecture • 3.4.1 - High availability 3.4.1.1 - Load balancing vs. clustering • 3.4.2 - Site considerations 3.4.2.4 - Geographic dispersion • 3.4.9 - Power 3.4.9.1 - Generators 3.4.9.2 - Uninterruptible power supply (UPS) 5.3 Explain the processes associated with third-party risk assessment and management • 5.3.2 - Vendor selection
9.5	Backup and Restore	3.4 Explain the importance of resilience and recovery in security architecture • 3.4.8 - Backups 3.4.8.1 - Onsite/offsite 3.4.8.2 - Frequency

		3.4.8.3 - Encryption 3.4.8.4 - Snapshots 3.4.8.5 - Recovery 3.4.8.6 - Replication 3.4.8.7 - Journaling
10.0	**Protocol, App, and Cloud Security**	
10.1	Host Virtualization	2.3 Explain various types of vulnerabilities • 2.3.5 - Virtualization 2.3.5.1 - Virtual machine (VM) escape 2.3.5.2 - Resource reuse 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.1 - Segmentation 3.1 Compare and contrast security implications of different architecture models • 3.1.1 - Architecture and infrastructure concepts 3.1.1.5 - Network infrastructure 3.1.1.5.2 - Logical segmentation 3.1.1.8 - Containerization 3.1.1.9 - Virtualization 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.1 - Infrastructure considerations 3.2.1.7.4 - Load balancer

		3.4 Explain the importance of resilience and recovery in security architecture • 3.4.1 - High availability 3.4.1.1 - Load balancing vs. clustering 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.7. Sandboxing 4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.1 - Vulnerability scan
10.2	Virtual Networking	3.1 Compare and contrast security implications of different architecture models • 3.1.1 - Architecture and infrastructure concepts 3.1.1.5 - Network infrastructure 3.1.1.9 - Virtualization 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.1 - Virtual private network (VPN) 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.7. Sandboxing

10.3	Software-Defined Networking	3.1 Compare and contrast security implications of different architecture models • 3.1.1 - Architecture and infrastructure concepts 3.1.1.5.3 - Software-defined networking (SDN)
10.4	Cloud Services	1.2 Summarize fundamental security concepts • 1.2.3 - Authentication, Authorization, and Accounting (AAA) 1.2.3.1 - Authenticating people 2.2 Explain common threat vectors and attack surfaces • 2.2.11 - Supply chain 2.2.11.1 - Managed service providers (MSPs) 2.2.11.2 - Vendors 2.2.11.3 - Suppliers 2.3 Explain various types of vulnerabilities • 2.3.6 - Cloud-specific • 2.3.7 - Supply chain 2.3.7.1 - Service provider 3.1 Compare and contrast security implications of different architecture models • 3.1.1 - Architecture and infrastructure concepts 3.1.1.1 - Cloud 3.1.1.1.2 - Hybrid considerations 3.1.1.1.3 - Third-party vendors

		3.1.1.3 - Serverless 3.1.1.9 - Virtualization • 3.1.2 - Considerations 3.4 Explain the importance of resilience and recovery in security architecture • 3.4.4 - Multi-cloud systems 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.2 - Hardening targets 4.1.2.5 - Cloud infrastructure 5.3 Explain the processes associated with third-party risk assessment and management • 5.3.1 - Vendor assessment 5.3.1.1 - Penetration testing 5.3.1.2 - Right-to-audit clause 5.3.1.4 - Independent assessments • 5.3.4 - Vendor monitoring
10.5	Mobile Devices	2.3 Explain various types of vulnerabilities • 2.3.10 - Mobile device 2.3.10.1 - Side loading 2.3.10.2 - Jailbreaking 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.3 - Application allow list

		• 2.5.11 - Hardening techniques 2.5.11.1 - Encryption 3.3 Compare and contrast concepts and strategies to protect data • 3.3.4 - Methods to secure data 3.3.4.2 - Encryption 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.1 - Secure baselines 4.1.1.1 - Establish 4.1.1.2 - Deploy • 4.1.2 - Hardening targets 4.1.2.1 - Mobile devices • 4.1.3. Wireless devices 4.1.3.1 - Installation considerations • 4.1.4 - Mobile solutions 4.1.4.1 - Mobile device management (MDM) 4.1.4.2 - Deployment models 4.1.4.2.1 - Bring your own device (BYOD) 4.1.4.2.2 - Corporate-owned, personally enabled (COPE) 4.1.4.2.3 - Choose your own device (CYOD) 4.1.4.3 - Connections methods 4.1.4.3.1 - Cellular 4.1.4.3.2 - Wi-Fi

		4.1.4.3.3 - Bluetooth • 4.1.6 - Application security 4.1.6.4 - Code signing • 4.1.7. Sandboxing 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.4 - Operating system security 4.5.4.1 - Group Policy 4.6 Given a scenario, implement and maintain identity and access management • 4.6.10 - Password concepts 4.6.10.2 - Password managers
10.6	Mobile Device Management	2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.3 - Application allow list 3.1 Compare and contrast security implications of different architecture models • 3.1.2 - Considerations 3.1.2.6 - Ease of deployment 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.4 - Mobile solutions

		4.1.4.1 - Mobile device management (MDM) 4.1.4.2 - Deployment models 4.1.4.2.1 - Bring your own device (BYOD) 4.2 Explain the security implications of proper hardware, software, and data asset management • 4.2.3 - Disposal/decommissioning 4.2.3.1 - Sanitization 4.2.3.2 - Destruction 4.2.3.4 - Data retention
10.7	BYOD Security	2.2 Explain common threat vectors and attack surfaces • 2.2.8 - Unsecure networks 2.2.8.1 - Wireless 2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.4 - Isolation 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.2 - Hardening targets 4.1.2.1 - Mobile devices • 4.1.3. Wireless devices 4.1.3.1 - Installation considerations • 4.1.4 - Mobile solutions

		4.1.4.1 - Mobile device management (MDM) 4.1.4.2 - Deployment models 4.1.4.2.1 - Bring your own device (BYOD) 4.1.4.2.2 - Corporate-owned, personally enabled (COPE) 4.1.4.2.3 - Choose your own device (CYOD) 4.1.4.3.2 - Wi-Fi 4.1.4.3.3 - Bluetooth 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.10. Network access control (NAC) 4.6 Given a scenario, implement and maintain identity and access management • 4.6.8 - Access controls 5.1 Summarize elements of effective security governance • 5.1.2 - Policies 5.1.2.1 - Acceptable use policy (AUP)
10.8	Embedded and Specialized Systems	1.4 Explain the importance of using appropriate cryptographic solutions • 1.4.3 - Tools 1.4.3.1 - Trusted Platform Module (TPM) 2.2 Explain common threat vectors and attack surfaces • 2.2.8 - Unsecure networks 2.2.8.1 - Wireless 2.2.8.2 - Wired

		2.2.8.3 - Bluetooth 3.1 Compare and contrast security implications of different architecture models • 3.1.1 - Architecture and infrastructure concepts 3.1.1.10 - IoT 3.1.1.11 - Industrial control systems (ICS)/supervisory control and data acquisition (SCADA) 3.1.1.12 - Real-time operating system (RTOS) 3.1.1.13 - Embedded systems 3.3 Compare and contrast concepts and strategies to protect data • 3.3.4 - Methods to secure data 3.3.4.2 - Encryption 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.2 - Hardening targets 4.1.2.1 - Mobile devices 4.1.2.7 - ICS/SCADA 4.1.2.8 - Embedded systems 4.1.2.10 - IoT devices • 4.1.4 - Mobile solutions 4.1.4.3.1 - Cellular 4.1.4.3.2 - Wi-Fi 4.1.4.3.3 - Bluetooth
10.9	Email	2.4 Given a scenario, analyze indicators of malicious activity

		• 2.4.1 - Malware attacks 2.4.1.6 - Virus • 2.4.4 - Application attacks 3.2 Given a scenario, apply security principles to secure enterprise infrastructure • 3.2.2 - Secure communication/access 3.2.2.3.1 - Transport Layer Security (TLS) 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.6 - Application security 4.1.6.2 - Secure cookies 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.7 - Email security 4.5.7.1 - Domain-based Message Authentication Reporting and Conformance (DMARC) 4.5.7.2 - DomainKeys Identified Mail (DKIM) 4.5.7.3 - Sender Policy Framework (SPF) 4.5.7.4 - Gateway • 4.5.9. DLP 5.6 Given a scenario, implement security awareness practices • 5.6.1 - Phishing

11.0	Security Governance Concepts	
11.1	Policies, Standards, and Procedures	4.6 Given a scenario, implement and maintain identity and access management • 4.6.9 - Multifactor authentication • 4.6.10 - Password concepts 4.6.10.1.1 - Length 4.6.10.1.2 - Complexity 4.6.10.1.3 - Reuse 4.6.10.1.4 - Expiration 5.1 Summarize elements of effective security governance • 5.1.1 - Guidelines • 5.1.2 - Policies 5.1.2.1 - Acceptable use policy (AUP) 5.1.2.2 - Information security policies 5.1.2.3 - Business continuity 5.1.2.4 - Disaster recovery 5.1.2.5 - Incident response 5.1.2.6 - Software development lifecycle (SDLC) 5.1.2.7 - Change management • 5.1.3 - Standards 5.1.3.1 - Password 5.1.3.2 - Access control 5.1.3.3 - Physical security 5.1.3.4 - Encryption • 5.1.4 - Procedures

		5.1.4.3 - Playbooks • 5.1.5 - External considerations 5.1.5.1 - Regulatory 5.1.5.2 - Legal 5.1.5.3 - Industry 5.1.5.4 - Local/regional 5.1.5.5 - National 5.1.5.6 - Global • 5.1.6 - Monitoring and revision • 5.1.7 - Types of governance structures 5.1.7.1 - Boards 5.1.7.2 - Committees 5.1.7.3 - Government entities 5.1.7.4 - Centralized/decentralized
11.2	Change Management	1.3 Explain the importance of change management processes and the impact to security • 1.3.2 - Technical implications 1.3.2.1 - Allow lists/deny lists 1.3.2.2 - Restricted activities 1.3.2.3 - Downtime 1.3.2.4 - Service restart 1.3.2.5 - Application restart 1.3.2.6 - Legacy applications 1.3.2.7 - Dependencies • 1.3.3 - Documentation 1.3.3.1 - Updating diagrams

		1.3.3.2 - Updating policies/procedures • 1.3.4 -Version control 5.1 Summarize elements of effective security governance • 5.1.2 - Policies 5.1.2.7 - Change management • 5.1.4 - Procedures 5.1.4.1 - Change management • 5.1.7 - Types of governance structures 5.1.7.1 - Boards 5.2 Explain elements of the risk management process • 5.2.3 - Risk analysis
11.3	Automation and Orchestration	4.7 Explain the importance of automation and orchestration related to secure operations • 4.7.1 - Use cases of automation and scripting 4.7.1.5 - Ticket creation 4.7.1.7 - Enabling/disabling services and access 4.7.1.8 - Continuous integration and testing • 4.7.2 - Benefits 4.7.2.1 - Efficiency/time saving 4.7.2.2 - Enforcing baselines 4.7.2.3 - Standard infrastructure configurations

		4.7.2.5 - Staff retention 4.7.2.6 - Reaction time 4.7.2.7 - Workforce multiplier • 4.7.3 - Other considerations 4.7.3.1 - Complexity 4.7.3.2 - Cost 4.7.3.3 - Single point of failure 4.7.3.4 - Technical debt 4.7.3.5 - Ongoing supportability
12.0	**Risk Management Processes**	
12.1	Risk Management Processes and Concepts	3.4 Explain the importance of resilience and recovery in security architecture • 3.4.1 - High availability • 3.4.2 - Site considerations 3.4.2.1 - Hot 3.4.2.2 - Cold 3.4.2.3 - Warm 3.4.2.4 - Geographic dispersion • 3.4.3 - Platform diversity • 3.4.4 - Multi-cloud systems • 3.4.5 - Continuity of operations • 3.4.6 - Capacity planning 3.4.6.1 - People 3.4.6.2 - Technology 3.4.6.3 - Infrastructure

		• 3.4.7 - Testing 3.4.7.1 - Tabletop exercises 3.4.7.2 - Fail over 3.4.7.3 - Simulation 3.4.7.4 - Parallel processing • 3.4.8 - Backups 4.2 Explain the security implications of proper hardware, software, and data asset management • 4.2.2 - Assignment/accounting 5.1 Summarize elements of effective security governance • 5.1.2 - Policies 5.1.2.3 - Business continuity 5.1.2.5 - Incident response 5.2 Explain elements of the risk management process • 5.2.1 - Risk identification • 5.2.2 - Risk assessment 5.2.2.1 - Ad hoc 5.2.2.2 - Recurring 5.2.2.3 - One-time 5.2.2.4 - Continuous • 5.2.3 - Risk analysis 5.2.3.1 - Qualitative 5.2.3.2 - Quantitative

		5.2.3.3 - Single loss expectancy (SLE) 5.2.3.4 - Annualized loss expectancy (ALE) 5.2.3.5 - Annualized rate of occurrence (ARO) 5.2.3.6 - Probability 5.2.3.7 - Likelihood 5.2.3.8 - Exposure factor 5.2.3.9 - Impact • 5.2.4 - Risk register 5.2.4.1 - Key risk indicators 5.2.4.2 - Risk owners 5.2.4.3 - Risk threshold • 5.2.5 - Risk tolerance • 5.2.6 - Risk appetite 5.2.6.1 - Expansionary 5.2.6.2 - Conservative 5.2.6.3 - Neutral • 5.2.7 - Risk management strategies 5.2.7.1 - Transfer 5.2.7.2 - Accept 5.2.7.2.1 - Exemption 5.2.7.2.2 - Exception 5.2.7.3 - Avoid 5.2.7.4 - Mitigate • 5.2.8 - Risk reporting • 5.2.9 - Business impact analysis 5.2.9.1 - Recovery time objective (RTO) 5.2.9.2 - Recovery point objective (RPO) 5.2.9.3 - Mean time to repair (MTTR)

		5.2.9.4 - Mean time between failures (MTBF)
12.2	Vendor Management	5.1 Summarize elements of effective security governance • 5.1.4 - Procedures 5.1.4.2 - Onboarding/offboarding 5.3 Explain the processes associated with third-party risk assessment and management • 5.3.1 - Vendor assessment 5.3.1.1 - Penetration testing 5.3.1.2 - Right-to-audit clause 5.3.1.3 - Evidence of internal audits 5.3.1.4 - Independent assessments 5.3.1.5 - Supply chain analysis • 5.3.2 - Vendor selection 5.3.2.1 - Due diligence 5.3.2.2 - Conflict of interest • 5.3.3 - Agreement types 5.3.3.1 - Service-level agreement (SLA) 5.3.3.2 - Memorandum of agreement (MOA) 5.3.3.3 - Memorandum of understanding (MOU) 5.3.3.4 - Master service agreement (MSA) 5.3.3.5 - Work order (WO)/statement of work (SOW) 5.3.3.6 - Non-disclosure agreement (NDA) 5.3.3.7 - Business partners agreement (BPA) • 5.3.4 - Vendor monitoring

		• 5.3.5 - Questionnaires • 5.3.6 - Rules of engagement
12.3	Audits and Assessments	4.3 Explain various activities associated with vulnerability management • 4.3.1 - Identification methods 4.3.1.6 - System/process audit • 4.3.4 - Validation of remediation 4.3.4.2 - Audit 4.4 Explain security alerting and monitoring concepts and tools • 4.4.2 - Activities 4.4.2.1 - Log aggregation 4.5 Given a scenario, modify enterprise capabilities to enhance security • 4.5.4 - Operating system security 4.5.4.1 - Group Policy 4.9 Given a scenario, use data sources to support an investigation • 4.9.1 - Log data 4.9.1.4 - OS-specific security logs 4.9.1.6 - Network logs 5.1 Summarize elements of effective security governance

		• 5.1.2 - Policies 5.1.2.2 - Information security policies 5.5 Explain types and purposes of audits and assessments • 5.5.1 - Attestation • 5.5.2 - Internal 5.5.2.1 - Compliance 5.5.2.2 - Audit committee 5.5.2.3 - Self-assessments • 5.5.3 - External 5.5.3.1 - Regulatory 5.5.3.2 - Examinations 5.5.3.3 - Assessment 5.5.3.4 - Independent third-party audit
13.0	**Data Protection and Compliance**	
13.1	Data Classification and Compliance	3.3 Compare and contrast concepts and strategies to protect data • 3.3.1 - Data types 3.3.1.1 - Regulated 3.3.1.2 - Trade secret 3.3.1.3 - Intellectual property 3.3.1.4 - Legal information 3.3.1.5 - Financial information 3.3.1.6 - Human and non-human readable • 3.3.2 - Data classifications

		3.3.2.1 - Sensitive 3.3.2.2 - Confidential 3.3.2.3 - Public 3.3.2.4 - Restricted 3.3.2.5 - Private 3.3.2.6 - Critical • 3.3.3 - General data considerations 3.3.3.2 - Data sovereignty 4.2 Explain the security implications of proper hardware, software, and data asset management • 4.2.3 - Disposal/decommissioning 4.2.3.1 - Sanitization 4.2.3.2 - Destruction 4.2.3.3 - Certification 4.2.3.4 - Data retention 5.1 Summarize elements of effective security governance • 5.1.8 - Roles and responsibilities for systems and data 5.1.8.2 - Controllers 5.1.8.3 - Processors 5.4 Summarize elements of effective security compliance • 5.4.2 - Consequences of non-compliance 5.4.2.1 - Fines 5.4.2.2 - Sanctions 5.4.2.3 - Reputational damage

		5.4.2.4 - Loss of license 5.4.2.5 - Contractual impacts • 5.4.4 - Privacy 5.4.4.1 - Legal implications 5.4.4.1.1 - Local/regional 5.4.4.1.2 - National 5.4.4.1.3 - Global 5.4.4.2 - Data subject 5.4.4.3 - Controller vs. processor 5.4.4.4 - Ownership 5.4.4.5 - Data inventory and retention 5.4.4.6 - Right to be forgotten
13.2	Personnel Policies	2.5 Explain the purpose of mitigation techniques used to secure the enterprise • 2.5.8 - Least privilege 3.3 Compare and contrast concepts and strategies to protect data • 3.3.1 - Data types 3.3.1.1 - Regulated 3.3.1.3 - Intellectual property 3.3.1.4 - Legal information 3.3.1.5 - Financial information • 3.3.2 - Data classifications • 3.3.3 - General data considerations 3.3.3.1 - Data states 3.3.3.1.1 - Data at rest 3.3.3.1.2 - Data in transit 3.3.3.1.3 - Data in use 3.3.3.2 - Data sovereignty

		3.3.3.3 - Geolocation • 3.3.4 - Methods to secure data 3.3.4.2 - Encryption 4.1 Given a scenario, apply common security techniques to computing resources • 4.1.4 - Mobile solutions 4.1.4.2.1 - Bring your own device (BYOD) 4.2 Explain the security implications of proper hardware, software, and data asset management • 4.2.3 - Disposal/decommissioning 4.2.3.4 - Data retention 4.4 Explain security alerting and monitoring concepts and tools • 4.4.3 - Tools 4.4.3.3.3 - Data loss prevention (DLP) 4.6 Given a scenario, implement and maintain identity and access management • 4.6.8 - Access controls 4.6.8.7 - Least privilege 4.8 Explain appropriate incident response activities • 4.8.2 - Training

		• 4.8.6 - Digital forensics 4.8.6.1 - Legal hold 5.1 Summarize elements of effective security governance • 5.1.2 - Policies 5.1.2.1 - Acceptable use policy (AUP) • 5.1.4 - Procedures 5.1.4.2 - Onboarding/offboarding 5.3 Explain the processes associated with third-party risk assessment and management • 5.3.2 - Vendor selection 5.3.2.1 - Due diligence 5.4 Summarize elements of effective security compliance • 5.4.4 - Privacy 5.4.4.1 - Legal implications 5.4.4.5 - Data inventory and retention 5.6 Given a scenario, implement security awareness practices • 5.6.1 - Phishing 5.6.1.2 - Recognizing a phishing attempt • 5.6.2 - Anomalous behavior recognition

		5.6.2.1 - Risky 5.6.2.2 - Unexpected 5.6.2.3 - Unintentional • 5.6.3 - User guidance and training 5.6.3.1 - Policy/handbooks 5.6.3.2 - Situational awareness 5.6.3.5 - Removable media and cables 5.6.3.6 - Social engineering • 5.6.4 - Reporting and monitoring 5.6.4.1 - Initial 5.6.4.2 - Recurring • 5.6.5 - Development
A.0	**CompTIA Security+ SY0-701 - Practice Exams**	
A.1	Prepare for CompTIA Security+ SY0-701 Certification	
A.2	CompTIA Security+ Domain Review (20 Questions)	
A.3	CompTIA Security+ Domain Review (All Questions)	
B.0	**TestOut Security Pro - Practice Exams**	

B.1	Prepare for TestOut Security Pro Certification	
B.2	TestOut Security Pro Domain Review	

Objective Mapping: CompTIA SY0-701 Objective to LabSim Section

#	Domain	Module.Section
1.0	**General Security Concepts**	
1.1	Compare and contrast various types of security controls 1.1.1 - Categories ○ 1.1.1.1 - Technical ○ 1.1.1.2 - Managerial ○ 1.1.1.3 - Operational ○ 1.1.1.4 - Physical 1.1.2 - Control types ○ 1.1.2.1 - Preventive ○ 1.1.2.2 - Deterrent ○ 1.1.2.3 - Detective ○ 1.1.2.4 - Corrective ○ 1.1.2.5 - Compensating ○ 1.1.2.6 - Directive	1.1, 1.2 5.10 7.1
1.2	Summarize fundamental security concepts 1.2.1 - Confidentiality, Integrity, and Availability (CIA) 1.2.2 - Non-repudiation 1.2.3 - Authentication, Authorization, and Accounting (AAA) ○ 1.2.3.1 - Authenticating people ○ 1.2.3.2 - Authenticating systems ○ 1.2.3.3 - Authorization models 1.2.4 - Gap analysis 1.2.5 - Zero trust ○ 1.2.5.1 - Control plane ○ 1.2.5.1.1 - Adaptive identity ○ 1.2.5.1.2 - Threat scope reduction ○ 1.2.5.1.3 - Policy-driven access control ○ 1.2.5.1.4 - Policy Administrator ○ 1.2.5.1.5 - Policy Engine	1.1 4.1, 4.2, 4.3, 4.4, 4.5 5.2 6.1 8.2 10.4

	○ 1.2.5.2 - Data plane ○ 1.2.5.2.1 - Implicit trust zones ○ 1.2.5.2.2 - Subject/System ○ 1.2.5.2.3 - Policy enforcement point 1.2.6 - Physical security ○ 1.2.6.1 - Bollards ○ 1.2.6.2 - Access control vestibule ○ 1.2.6.3 - Fencing ○ 1.2.6.4 - Video surveillance ○ 1.2.6.5 - Security guard ○ 1.2.6.6 - Access badge ○ 1.2.6.7 - Lighting ○ 1.2.6.8 - Sensors ○ 1.2.6.8.1 - Infrared ○ 1.2.6.8.2 - Pressure ○ 1.2.6.8.3 - Microwave ○ 1.2.6.8.4 - Ultrasonic 1.2.7 - Deception and disruption technology ○ 1.2.7.1 - Honeypot ○ 1.2.7.2 - Honeynet ○ 1.2.7.3 - Honeyfile ○ 1.2.7.4 - Honeytoken	
1.3	Explain the importance of change management processes and the impact to security 1.3.1 - Business processes impacting security operation ○ 1.3.1.1 - Approval process ○ 1.3.1.2 - Ownership ○ 1.3.1.3 - Stakeholders ○ 1.3.1.4 - Impact analysis ○ 1.3.1.5 - Test results ○ 1.3.1.6 - Backout plan ○ 1.3.1.7 - Maintenance window ○ 1.3.1.8 - Standard operating procedure 1.3.2 - Technical implications ○ 1.3.2.1 - Allow lists/deny lists ○ 1.3.2.2 - Restricted activities ○ 1.3.2.3 - Downtime	8.9 11.2

	○ 1.3.2.4 - Service restart ○ 1.3.2.5 - Application restart ○ 1.3.2.6 - Legacy applications ○ 1.3.2.7 - Dependencies 1.3.3 - Documentation ○ 1.3.3.1 - Updating diagrams ○ 1.3.3.2 - Updating policies/procedures 1.3.4 -Version control	
1.4	Explain the importance of using appropriate cryptographic solutions 1.4.1 - Public key infrastructure (PKI) ○ 1.4.1.1 - Public key ○ 1.4.1.2 - Private key ○ 1.4.1.3 - Key escrow 1.4.2 - Encryption ○ 1.4.2.1 - Level ○ 1.4.2.1.1 - Full-disk ○ 1.4.2.1.2 - Partition ○ 1.4.2.1.3 - File ○ 1.4.2.1.4 - Volume ○ 1.4.2.1.5 - Database ○ 1.4.2.1.6 - Record ○ 1.4.2.2 - Transport/communication ○ 1.4.2.3 - Asymmetric ○ 1.4.2.4 - Symmetric ○ 1.4.2.5 - Key exchange ○ 1.4.2.6 - Algorithms ○ 1.4.2.7 - Key length 1.4.3 - Tools ○ 1.4.3.1 - Trusted Platform Module (TPM) ○ 1.4.3.2 - Hardware security module (HSM) ○ 1.4.3.3 - Key management system ○ 1.4.3.4 - Secure enclave 1.4.4 - Obfuscation ○ 1.4.4.1 - Steganography ○ 1.4.4.2 - Tokenization ○ 1.4.4.3 - Data masking	3.1, 3.2, 3.3, 3.4, 3.5 4.3 5.8 6.6 7.3 8.1, 8.2, 8.7 10.8

	1.4.5 - Hashing 1.4.6 - Salting 1.4.7 - Digital signatures 1.4.8 - Key stretching 1.4.9 - Blockchain 1.4.10 - Open public ledger 1.4.11 - Certificates ○ 1.4.11.1 - Certificate authorities ○ 1.4.11.2 - Certificate revocation lists (CRLs) ○ 1.4.11.3 - Online Certificate Status Protocol (OCSP) ○ 1.4.11.4 - Self-signed ○ 1.4.11.5 - Third-party ○ 1.4.11.6 - Root of trust ○ 1.4.11.7 - Certificate signing request (CSR) generation ○ 1.4.11.8 - Wildcard	
2.0	**Threats, Vulnerabilities, and Mitigations**	
2.1	Compare and contrast common threat actors and motivations 2.1.1 - Threat actors ○ 2.1.1.1 - Nation-state ○ 2.1.1.2 - Unskilled attacker ○ 2.1.1.3 - Hacktivist ○ 2.1.1.4 - Insider threat ○ 2.1.1.5 - Organized crime ○ 2.1.1.6 - Shadow IT 2.1.2 - Attributes of actors ○ 2.1.2.1 - Internal/external ○ 2.1.2.2 - Resources/funding ○ 2.1.2.3 - Level of sophistication/capability 2.1.3 - Motivations ○ 2.1.3.1 - Data exfiltration ○ 2.1.3.2 - Espionage ○ 2.1.3.3 - Service disruption ○ 2.1.3.4 - Blackmail ○ 2.1.3.5 - Financial gain	1.1 2.1, 2.2 6.5

	○ 2.1.3.6 - Philosophical/political beliefs ○ 2.1.3.7- Ethical ○ 2.1.3.8 - Revenge ○ 2.1.3.9 - Disruption/chaos ○ 2.1.3.10 - War	
2.2	Explain common threat vectors and attack surfaces 2.2.1 - Message-based ○ 2.2.1.1 - Email ○ 2.2.1.2 - Short Message Service (SMS) ○ 2.2.1.3 - Instant messaging (IM) 2.2.2 - Image-based 2.2.3 - File-based 2.2.4 - Voice call 2.2.5 - Removable device 2.2.6 - Vulnerable software ○ 2.2.6.1 - Client-based vs. agentless 2.2.7 - Unsupported systems and applications 2.2.8 - Unsecure networks ○ 2.2.8.1 - Wireless ○ 2.2.8.2 - Wired ○ 2.2.8.3 - Bluetooth 2.2.9 - Open service ports 2.2.10 - Default credentials 2.2.11 - Supply chain ○ 2.2.11.1 - Managed service providers (MSPs) ○ 2.2.11.2 - Vendors ○ 2.2.11.3 - Suppliers 2.2.12 - Human vectors/social engineering ○ 2.2.12.1 - Phishing ○ 2.2.12.2 - Vishing ○ 2.2.12.3 - Smishing ○ 2.2.12.4 - Misinformation/disinformation ○ 2.2.12.5 - Impersonation ○ 2.2.12.6 - Business email compromise ○ 2.2.12.7 - Pretexting ○ 2.2.12.8 - Watering hole	2.1, 2.2 5.10 6.2, 6.6 7.2, 7.4 8.1, 8.2, 8.3, 8.5, 8.6, 8.9 10.4, 10.7, 10.8

	○ 2.2.12.9 - Brand impersonation ○ 2.2.12.10 - Typosquatting	
2.3	Explain various types of vulnerabilities 2.3.1 - Application ○ 2.3.1.1 - Memory injection ○ 2.3.1.2 - Buffer overflow ○ 2.3.1.3 - Race conditions ○ 2.3.1.3.1 - Time-of-check (TOC) ○ 2.3.1.3.2 - Time-of-use (TOU) ○ 2.3.1.4 - Malicious update 2.3.2 - Operating system (OS)-based 2.3.3 - Web-based ○ 2.3.3.1 - Structured Query Language injection (SQLi) ○ 2.3.3.2 - Cross-site scripting (XSS) 2.3.4 - Hardware ○ 2.3.4.1 - Firmware ○ 2.3.4.2 - End-of-life ○ 2.3.4.3 - Legacy 2.3.5 - Virtualization ○ 2.3.5.1 - Virtual machine (VM) escape ○ 2.3.5.2 - Resource reuse 2.3.6 - Cloud-specific 2.3.7 - Supply chain ○ 2.3.7.1 - Service provider ○ 2.3.7.2 - Hardware provider ○ 2.3.7.3 - Software provider 2.3.8 - Cryptographic 2.3.9 - Misconfiguration 2.3.10 - Mobile device ○ 2.3.10.1 - Side loading ○ 2.3.10.2 - Jailbreaking 2.3.11 - Zero-day	2.1 5.7, 5.10 7.1 8.6, 8.8 10.1, 10.4, 10.5
2.4	Given a scenario, analyze indicators of malicious activity	2.1, 2.3

	2.4.1 - Malware attacks ○ 2.4.1.1 - Ransomware ○ 2.4.1.2 - Trojan ○ 2.4.1.3 - Worm ○ 2.4.1.4 - Spyware ○ 2.4.1.5 - Bloatware ○ 2.4.1.6 - Virus ○ 2.4.1.7 - Keylogger ○ 2.4.1.8 - Logic bomb ○ 2.4.1.9 - Rootkit 2.4.2 - Physical attacks ○ 2.4.2.1 - Brute force ○ 2.4.2.2 - Radio frequency identification (RFID) cloning ○ 2.4.2.3 - Environmental 2.4.3 - Network attacks ○ 2.4.3.1 - Distributed denial-of-service (DDoS) ○ 2.4.3.1.1 - Amplified ○ 2.4.3.1.2 - Reflected ○ 2.4.3.2 - Domain Name System (DNS) attacks ○ 2.4.3.3 - Wireless ○ 2.4.3.4 - On-path ○ 2.4.3.5 - Credential replay ○ 2.4.3.6 - Malicious code 2.4.4 - Application attacks ○ 2.4.4.1 - Injection ○ 2.4.4.2 - Buffer overflow ○ 2.4.4.3 - Replay ○ 2.4.4.4 - Privilege escalation ○ 2.4.4.5 - Forgery ○ 2.4.4.6 - Directory traversal 2.4.5 - Cryptographic attacks ○ 2.4.5.1 - Downgrade ○ 2.4.5.2 - Collision ○ 2.4.5.3 - Birthday 2.4.6 - Password attacks ○ 2.4.6.1 - Spraying ○ 2.4.6.2 - Brute force 2.4.7 - Indicators ○ 2.4.7.1 - Account lockout	3.1 4.5 5.7 6.1, 6.4, 6.5, 6.6 8.5, 8.7, 8.8 10.9

	○ 2.4.7.2 - Concurrent session usage ○ 2.4.7.3 - Blocked content ○ 2.4.7.4 - Impossible travel ○ 2.4.7.5 - Resource consumption ○ 2.4.7.6 - Resource inaccessibility ○ 2.4.7.7 - Out-of-cycle logging ○ 2.4.7.8 - Published/documented ○ 2.4.7.9 - Missing logs	
2.5	Explain the purpose of mitigation techniques used to secure the enterprise 2.5.1 - Segmentation 2.5.2 - Access control ○ 2.5.2.1 - Access control list (ACL) ○ 2.5.2.2 - Permissions 2.5.3 - Application allow list 2.5.4 - Isolation 2.5.5 - Patching 2.5.6 - Encryption 2.5.7 - Monitoring 2.5.8 - Least privilege 2.5.9 - Configuration enforcement 2.5.10 - Decommissioning 2.5.11 - Hardening techniques ○ 2.5.11.1 - Encryption ○ 2.5.11.2 - Installation of endpoint protection ○ 2.5.11.3 - Host-based firewall ○ 2.5.11.4 - Host-based intrusion prevention system (HIPS) ○ 2.5.11.5 - Disabling ports/protocols ○ 2.5.11.6 - Default password changes ○ 2.5.11.7 - Removal of unnecessary software	2.1 3.4 4.1, 4.3, 4.6 5.4, 5.7, 5.10 6.2, 6.3, 6.4 7.3 8.1, 8.2, 8.3, 8.6, 8.8, 8.9 9.1, 9.2 10.1, 10.5, 10.6, 10.7 13.2
3.0	**Security Architecture**	
3.1	Compare and contrast security implications of different architecture models	5.1 9.4

	3.1.1 - Architecture and infrastructure concepts ○ 3.1.1.1 - Cloud ○ 3.1.1.1.1 - Responsibility matrix ○ 3.1.1.1.2 - Hybrid considerations ○ 3.1.1.1.3 - Third-party vendors ○ 3.1.1.2 - Infrastructure as code (IaC) ○ 3.1.1.3 - Serverless ○ 3.1.1.4 - Microservices ○ 3.1.1.5 - Network infrastructure ○ 3.1.1.5.1 - Physical isolation ○ 3.1.1.5.1.1 - Air-gapped ○ 3.1.1.5.2 - Logical segmentation ○ 3.1.1.5.3 - Software-defined networking (SDN) ○ 3.1.1.6 - On-premises ○ 3.1.1.7 - Centralized/decentralized ○ 3.1.1.8 - Containerization ○ 3.1.1.9 - Virtualization ○ 3.1.1.10 - IoT ○ 3.1.1.11 - Industrial control systems (ICS)/supervisory control and data acquisition (SCADA) ○ 3.1.1.12 - Real-time operating system (RTOS) ○ 3.1.1.13 - Embedded systems ○ 3.1.1.14 - High availability 3.1.2 - Considerations ○ 3.1.2.1 - Availability ○ 3.1.2.2 - Resilience ○ 3.1.2.3 - Cost ○ 3.1.2.4 - Responsiveness ○ 3.1.2.5 - Scalability ○ 3.1.2.6 - Ease of deployment ○ 3.1.2.7 - Risk transference ○ 3.1.2.8 - Ease of recovery ○ 3.1.2.9 - Patch availability ○ 3.1.2.10 - Inability to patch ○ 3.1.2.11 - Power ○ 3.1.2.12 - Compute	10.1, 10.2, 10.3, 10.4, 10.6, 10.8

3.2	Given a scenario, apply security principles to secure enterprise infrastructure 3.2.1 - Infrastructure considerations ○ 3.2.1.1 - Device placement ○ 3.2.1.2 - Security zones ○ 3.2.1.3 - Attack surface ○ 3.2.1.4 - Connectivity ○ 3.2.1.5 - Failure modes ○ 3.2.1.5.1 - Fail-open ○ 3.2.1.5.2 - Fail-closed ○ 3.2.1.6 - Device attribute ○ 3.2.1.6.1 - Active vs. passive ○ 3.2.1.6.2 - Inline vs. tap/monitor ○ 3.2.1.7 - Network appliances ○ 3.2.1.7.1 - Jump server ○ 3.2.1.7.2 - Proxy server ○ 3.2.1.7.3 - Intrusion prevention system (IPS)/intrusion detection system (IDS) ○ 3.2.1.7.4 - Load balancer ○ 3.2.1.7.5 - Sensors ○ 3.2.1.8 - Port security ○ 3.2.1.8.1 - 802.1X ○ 3.2.1.8.2 - Extensible Authentication Protocol (EAP) ○ 3.2.1.9 - Firewall types ○ 3.2.1.9.1 - Web application firewall (WAF) ○ 3.2.1.9.2 - Unified threat management (UTM) ○ 3.2.1.9.3 - Next-generation firewall (NGFW) ○ 3.2.1.9.4 - Layer 4/Layer 7 3.2.2 - Secure communication/access ○ 3.2.2.1 - Virtual private network (VPN) ○ 3.2.2.2 - Remote access ○ 3.2.2.3 - Tunneling ○ 3.2.2.3.1 - Transport Layer Security (TLS) ○ 3.2.2.3.2 - Internet protocol security (IPSec) ○ 3.2.2.4 - Software-defined wide area network (SD-WAN) ○ 3.2.2.5 - Secure access service edge (SASE) 3.2.3 - Selection of effective controls	2.1 4.8 5.1, 5.2, 5.3, 5.4, 5.5, 5.9, 5.10 6.3 7.3 8.2, 8.6, 8.7, 8.8 9.2, 9.4 10.1, 10.2, 10.9

3.3	Compare and contrast concepts and strategies to protect data 3.3.1 - Data types ○ 3.3.1.1 - Regulated ○ 3.3.1.2 - Trade secret ○ 3.3.1.3 - Intellectual property ○ 3.3.1.4 - Legal information ○ 3.3.1.5 - Financial information ○ 3.3.1.6 - Human and non-human readable 3.3.2 - Data classifications ○ 3.3.2.1 - Sensitive ○ 3.3.2.2 - Confidential ○ 3.3.2.3 - Public ○ 3.3.2.4 - Restricted ○ 3.3.2.5 - Private ○ 3.3.2.6 - Critical 3.3.3 - General data considerations ○ 3.3.3.1 - Data states ○ 3.3.3.1.1 - Data at rest ○ 3.3.3.1.2 - Data in transit ○ 3.3.3.1.3 - Data in use ○ 3.3.3.2 - Data sovereignty ○ 3.3.3.3 - Geolocation 3.3.4 - Methods to secure data ○ 3.3.4.1 - Geographic restrictions ○ 3.3.4.2 - Encryption ○ 3.3.4.3 - Hashing ○ 3.3.4.4 - Masking ○ 3.3.4.5 - Tokenization ○ 3.3.4.6 - Obfuscation ○ 3.3.4.7 - Segmentation ○ 3.3.4.8 - Permission restrictions	5.9, 5.10 7.3 8.9 10.5, 10.8 13.1, 13.2
3.4	Explain the importance of resilience and recovery in security architecture 3.4.1 - High availability ○ 3.4.1.1 - Load balancing vs. clustering 3.4.2 - Site considerations	6.1 9.4, 9.5 10.1, 10.4

	○ 3.4.2.1 - Hot ○ 3.4.2.2 - Cold ○ 3.4.2.3 - Warm ○ 3.4.2.4 - Geographic dispersion 3.4.3 - Platform diversity 3.4.4 - Multi-cloud systems 3.4.5 - Continuity of operations 3.4.6 - Capacity planning ○ 3.4.6.1 - People ○ 3.4.6.2 - Technology ○ 3.4.6.3 - Infrastructure 3.4.7 - Testing ○ 3.4.7.1 - Tabletop exercises ○ 3.4.7.2 - Fail over ○ 3.4.7.3 - Simulation ○ 3.4.7.4 - Parallel processing 3.4.8 - Backups ○ 3.4.8.1 - Onsite/offsite ○ 3.4.8.2 - Frequency ○ 3.4.8.3 - Encryption ○ 3.4.8.4 - Snapshots ○ 3.4.8.5 - Recovery ○ 3.4.8.6 - Replication ○ 3.4.8.7 - Journaling 3.4.9 - Power ○ 3.4.9.1 - Generators ○ 3.4.9.2 - Uninterruptible power supply (UPS)	12.1
4.0	**Security Operations**	
4.1	Given a scenario, apply common security techniques to computing resources 4.1.1 - Secure baselines ○ 4.1.1.1 - Establish ○ 4.1.1.2 - Deploy ○ 4.1.1.3 - Maintain 4.1.2 - Hardening targets	3.5 4.6, 4.8 5.9, 5.10 6.2, 6.4 7.3

	○ 4.1.2.1 - Mobile devices ○ 4.1.2.2 - Workstations ○ 4.1.2.3 - Switches ○ 4.1.2.4 - Routers ○ 4.1.2.5 - Cloud infrastructure ○ 4.1.2.6 - Servers ○ 4.1.2.7 - ICS/SCADA ○ 4.1.2.8 - Embedded systems ○ 4.1.2.9 - RTOS ○ 4.1.2.10 - IoT devices 4.1.3. Wireless devices ○ 4.1.3.1 - Installation considerations ○ 4.1.3.1.1 - Site surveys ○ 4.1.3.1.2 - Heat maps 4.1.4 - Mobile solutions ○ 4.1.4.1 - Mobile device management (MDM) ○ 4.1.4.2 - Deployment models ○ 4.1.4.2.1 - Bring your own device (BYOD) ○ 4.1.4.2.2 - Corporate-owned, personally enabled (COPE) ○ 4.1.4.2.3 - Choose your own device (CYOD) ○ 4.1.4.3 - Connections methods ○ 4.1.4.3.1 - Cellular ○ 4.1.4.3.2 - Wi-Fi ○ 4.1.4.3.3 - Bluetooth 4.1.5 - Wireless security settings ○ 4.1.5.1 - Wi-Fi Protected Access 3 (WPA3) ○ 4.1.5.2 - AAA/Remote Authentication Dial-In User Service (RADIUS) ○ 4.1.5.3 - Cryptographic protocols ○ 4.1.5.4 - Authentication protocols 4.1.6 - Application security ○ 4.1.6.1 - Input validation ○ 4.1.6.2 - Secure cookies ○ 4.1.6.3 - Static code analysis ○ 4.1.6.4 - Code signing 4.1.7. Sandboxing 4.1.8. Monitoring	8.1, 8.2, 8.4, 8.5, 8.6, 8.8, 8.9 9.2 10.1, 10.2, 10.4, 10.5, 10.6, 10.7, 10.8, 10.9 13.2

4.2	Explain the security implications of proper hardware, software, and data asset management 4.2.1 - Acquisition/procurement process 4.2.2 - Assignment/accounting ○ 4.2.2.1 - Ownership ○ 4.2.2.2 - Classification 4.2.3 - Disposal/decommissioning ○ 4.2.3.1 - Sanitization ○ 4.2.3.2 - Destruction ○ 4.2.3.3 - Certification ○ 4.2.3.4 - Data retention	8.2 10.6 12.1 13.1, 13.2
4.3	Explain various activities associated with vulnerability management 4.3.1 - Identification methods ○ 4.3.1.1 - Vulnerability scan ○ 4.3.1.2 - Application security ○ 4.3.1.2.1 - Static analysis ○ 4.3.1.2.2 - Dynamic analysis ○ 4.3.1.2.3 - Package monitoring ○ 4.3.1.3 - Threat feed ○ 4.3.1.3.1 - Open-source intelligence (OSINT) ○ 4.3.1.3.2 - Proprietary/third-party ○ 4.3.1.3.3 - Information-sharing organization ○ 4.3.1.3.4 - Dark web ○ 4.3.1.4 - Penetration testing ○ 4.3.1.5 - Responsible disclosure program ○ 4.3.1.5.1 - Bug bounty program ○ 4.3.1.6 - System/process audit 4.3.2 - Analysis ○ 4.3.2.1 - Confirmation ○ 4.3.2.1.1 - False positive ○ 4.3.2.1.2 - False negative ○ 4.3.2.2 - Prioritize ○ 4.3.2.3 - Common Vulnerability Scoring System (CVSS) ○ 4.3.2.4 - Common Vulnerability Enumeration (CVE) ○ 4.3.2.5 - Vulnerability classification ○ 4.3.2.6 - Exposure factor	5.8 6.2, 6.3 7.1, 7.2, 7.3, 7.4 8.1, 8.2, 8.9 9.2 10.1 12.3

	○ 4.3.2.7 - Environmental variables ○ 4.3.2.8 - Industry/organizational impact ○ 4.3.2.9 - Risk tolerance 4.3.3 - Vulnerability response and remediation ○ 4.3.3.1 - Patching ○ 4.3.3.2 - Insurance ○ 4.3.3.3 - Segmentation ○ 4.3.3.4 - Compensating controls ○ 4.3.3.5 - Exceptions and exemptions 4.3.4 - Validation of remediation ○ 4.3.4.1 - Rescanning ○ 4.3.4.2 - Audit ○ 4.3.4.3 - Verification 4.3.5 - Reporting	
4.4	Explain security alerting and monitoring concepts and tools 4.4.1 - Monitoring computing resources ○ 4.4.1.1 - Systems ○ 4.4.1.2 - Applications ○ 4.4.1.3 - Infrastructure 4.4.2 - Activities ○ 4.4.2.1 - Log aggregation ○ 4.4.2.2 - Alerting ○ 4.4.2.3 - Scanning ○ 4.4.2.4 - Reporting ○ 4.4.2.5 - Archiving ○ 4.4.2.6 - Alert response and remediation/validation ○ 4.4.2.6.1 - Quarantine ○ 4.4.2.6.2 - Alert tuning 4.4.3 - Tools ○ 4.4.3.1 - Security Content Automation Protocol (SCAP) ○ 4.4.3.2 - Benchmarks ○ 4.4.3.3 - Agents/agentless ○ 4.4.3.3.1 - Security information and event management (SIEM) ○ 4.4.3.3.2 - Antivirus ○ 4.4.3.3.3 - Data loss prevention (DLP) ○ 4.4.3.4 - Simple Network Management Protocol (SNMP) traps	6.2 7.1, 7.2, 7.3, 7.4 9.2 12.3 13.2

	○ 4.4.3.5 - NetFlow ○ 4.4.3.6 - Vulnerability scanners	
4.5	Given a scenario, modify enterprise capabilities to enhance security 4.5.1 - Firewall ○ 4.5.1.1 - Rules ○ 4.5.1.2 - Access lists ○ 4.5.1.3 - Ports/protocols ○ 4.5.1.4 - Screened subnets 4.5.2 - IDS/IPS ○ 4.5.2.1 - Trends ○ 4.5.2.2 - Signatures 4.5.3 - Web filter ○ 4.5.3.1 - Agent-based ○ 4.5.3.2 - Centralized proxy ○ 4.5.3.3 - Universal Resource Locator (URL) scanning ○ 4.5.3.4 - Content categorization ○ 4.5.3.5 - Block rules ○ 4.5.3.6 - Reputation 4.5.4 - Operating system security ○ 4.5.4.1 - Group Policy ○ 4.5.4.2 - SELinux 4.5.5 - Implementation of secure protocols ○ 4.5.5.1 - Protocol selection ○ 4.5.5.2 - Port selection ○ 4.5.5.3 - Transport method 4.5.6 - DNS filtering 4.5.7 - Email security ○ 4.5.7.1 - Domain-based Message Authentication Reporting and Conformance (DMARC) ○ 4.5.7.2 - DomainKeys Identified Mail (DKIM) ○ 4.5.7.3 - Sender Policy Framework (SPF) ○ 4.5.7.4 - Gateway 4.5.8. File integrity monitoring 4.5.9. DLP 4.5.10. Network access control (NAC)	4.4, 4.5, 4.6 5.2, 5.3, 5.4, 5.6, 5.9, 5.10 6.2, 6.3, 6.4 8.1, 8.2, 8.9 10.5, 10.7, 10.9 12.3

	4.5.11. Endpoint detection and response (EDR)/extended detection and response (XDR) 4.5.12. User behavior analytics	
4.6	Given a scenario, implement and maintain identity and access management 4.6.1 - Provisioning/de-provisioning user accounts 4.6.2 - Permission assignments and implications 4.6.3 - Identity proofing 4.6.4 - Federation 4.6.5 - Single sign-on (SSO) ○ 4.6.5.1 - Lightweight Directory Access Protocol (LDAP) ○ 4.6.5.2 - Open authorization (OAuth) ○ 4.6.5.3 - Security Assertions Markup Language (SAML) 4.6.6 - Interoperability 4.6.7 - Attestation 4.6.8 - Access controls ○ 4.6.8.1 - Mandatory ○ 4.6.8.2 - Discretionary ○ 4.6.8.3 - Role-based ○ 4.6.8.4 - Rule-based ○ 4.6.8.5 - Attribute-based ○ 4.6.8.6 - Time-of-day restrictions ○ 4.6.8.7 - Least privilege 4.6.9 - Multifactor authentication ○ 4.6.9.1 - Implementations ○ 4.6.9.1.1 - Biometrics ○ 4.6.9.1.2 - Hard/soft authentication tokens ○ 4.6.9.1.3 - Security keys ○ 4.6.9.2 - Factors ○ 4.6.9.2.1 - Something you know ○ 4.6.9.2.2 - Something you have ○ 4.6.9.2.3 - Something you are ○ 4.6.9.2.4 - Somewhere you are 4.6.10 - Password concepts ○ 4.6.10.1 - Password best practices ○ 4.6.10.1.1 - Length ○ 4.6.10.1.2 - Complexity	4.1, 4.2, 4.3, 4.5, 4.6, 4.7, 4.9 5.7 6.1 8.1, 8.2, 8.8, 8.9 10.5, 10.7 11.1 13.2

	○ 4.6.10.1.3 - Reuse ○ 4.6.10.1.4 - Expiration ○ 4.6.10.1.5 - Age ○ 4.6.10.2 - Password managers ○ 4.6.10.3 - Passwordless 4.6.11 - Privileged access management tools ○ 4.6.11.1 - Just-in-time permissions ○ 4.6.11.2 - Password vaulting ○ 4.6.11.3 - Temporal accounts	
4.7	Explain the importance of automation and orchestration related to secure operations 4.7.1 - Use cases of automation and scripting ○ 4.7.1.1 - User provisioning ○ 4.7.1.2 - Resource provisioning ○ 4.7.1.3 - Guard rails ○ 4.7.1.4 - Security groups ○ 4.7.1.5 - Ticket creation ○ 4.7.1.6 - Escalation ○ 4.7.1.7 - Enabling/disabling services and access ○ 4.7.1.8 - Continuous integration and testing ○ 4.7.1.9 - Integrations and Application programming interfaces (APIs) 4.7.2 - Benefits ○ 4.7.2.1 - Efficiency/time saving ○ 4.7.2.2 - Enforcing baselines ○ 4.7.2.3 - Standard infrastructure configurations ○ 4.7.2.4 - Scaling in a secure manner ○ 4.7.2.5 - Staff retention ○ 4.7.2.6 - Reaction time ○ 4.7.2.7 - Workforce multiplier 4.7.3 - Other considerations ○ 4.7.3.1 - Complexity ○ 4.7.3.2 - Cost ○ 4.7.3.3 - Single point of failure ○ 4.7.3.4 - Technical debt ○ 4.7.3.5 - Ongoing supportability	6.5 8.1, 8.9 11.3

4.8	Explain appropriate incident response activities 4.8.1 - Process ○ 4.8.1.1 - Preparation ○ 4.8.1.2 - Detection ○ 4.8.1.3 - Analysis ○ 4.8.1.4 - Containment ○ 4.8.1.5 - Eradication ○ 4.8.1.6 - Recovery ○ 4.8.1.7 - Lessons learned 4.8.2 - Training 4.8.3 - Testing ○ 4.8.3.1 - Tabletop exercise ○ 4.8.3.2 - Simulation 4.8.4 - Root cause analysis 4.8.5 - Threat hunting 4.8.6 - Digital forensics ○ 4.8.6.1 - Legal hold ○ 4.8.6.2 - Chain of custody ○ 4.8.6.3 - Acquisition ○ 4.8.6.4 - Reporting ○ 4.8.6.5 - Preservation ○ 4.8.6.6 - E-discovery	7.1 9.1, 9.3 13.2
4.9	Given a scenario, use data sources to support an investigation 4.9.1 - Log data ○ 4.9.1.1 - Firewall logs ○ 4.9.1.2 - Application logs ○ 4.9.1.3 - Endpoint logs ○ 4.9.1.4 - OS-specific security logs ○ 4.9.1.5 - IPS/IDS logs ○ 4.9.1.6 - Network logs ○ 4.9.1.7 - Metadata 4.9.2 - Data sources ○ 4.9.2.1 - Vulnerability scans ○ 4.9.2.2 - Automated reports ○ 4.9.2.3 - Dashboards	6.2, 6.4, 6.5 7.1, 7.2, 7.3 9.2, 9.3 12.3

	○ 4.9.2.4 - Packet captures	
5.0	**Security Program Management and Oversight**	
5.1	Summarize elements of effective security governance 5.1.1 - Guidelines 5.1.2 - Policies ○ 5.1.2.1 - Acceptable use policy (AUP) ○ 5.1.2.2 - Information security policies ○ 5.1.2.3 - Business continuity ○ 5.1.2.4 - Disaster recovery ○ 5.1.2.5 - Incident response ○ 5.1.2.6 - Software development lifecycle (SDLC) ○ 5.1.2.7 - Change management 5.1.3 - Standards ○ 5.1.3.1 - Password ○ 5.1.3.2 - Access control ○ 5.1.3.3 - Physical security ○ 5.1.3.4 - Encryption 5.1.4 - Procedures ○ 5.1.4.1 - Change management ○ 5.1.4.2 - Onboarding/offboarding ○ 5.1.4.3 - Playbooks 5.1.5 - External considerations ○ 5.1.5.1 - Regulatory ○ 5.1.5.2 - Legal ○ 5.1.5.3 - Industry ○ 5.1.5.4 - Local/regional ○ 5.1.5.5 - National ○ 5.1.5.6 - Global 5.1.6 - Monitoring and revision 5.1.7 - Types of governance structures ○ 5.1.7.1 - Boards ○ 5.1.7.2 - Committees ○ 5.1.7.3 - Government entities ○ 5.1.7.4 - Centralized/decentralized	4.1 5.7, 5.10 7.3 8.9 9.1 10.7 11.1, 11.2 12.1, 12.2, 12.3 13.1, 13.2

	5.1.8 - Roles and responsibilities for systems and data ○ 5.1.8.1 - Owners ○ 5.1.8.2 - Controllers ○ 5.1.8.3 - Processors ○ 5.1.8.4 - Custodians/stewards	
5.2	Explain elements of the risk management process 5.2.1 - Risk identification 5.2.2 - Risk assessment ○ 5.2.2.1 - Ad hoc ○ 5.2.2.2 - Recurring ○ 5.2.2.3 - One-time ○ 5.2.2.4 - Continuous 5.2.3 - Risk analysis ○ 5.2.3.1 - Qualitative ○ 5.2.3.2 - Quantitative ○ 5.2.3.3 - Single loss expectancy (SLE) ○ 5.2.3.4 - Annualized loss expectancy (ALE) ○ 5.2.3.5 - Annualized rate of occurrence (ARO) ○ 5.2.3.6 - Probability ○ 5.2.3.7 - Likelihood ○ 5.2.3.8 - Exposure factor ○ 5.2.3.9 - Impact 5.2.4 - Risk register ○ 5.2.4.1 - Key risk indicators ○ 5.2.4.2 - Risk owners ○ 5.2.4.3 - Risk threshold 5.2.5 - Risk tolerance 5.2.6 - Risk appetite ○ 5.2.6.1 - Expansionary ○ 5.2.6.2 - Conservative ○ 5.2.6.3 - Neutral 5.2.7 - Risk management strategies ○ 5.2.7.1 - Transfer ○ 5.2.7.2 - Accept ○ 5.2.7.2.1 - Exemption ○ 5.2.7.2.2 - Exception	8.9 11.2 12.1

	○ 5.2.7.3 - Avoid ○ 5.2.7.4 - Mitigate 5.2.8 - Risk reporting 5.2.9 - Business impact analysis ○ 5.2.9.1 - Recovery time objective (RTO) ○ 5.2.9.2 - Recovery point objective (RPO) ○ 5.2.9.3 - Mean time to repair (MTTR) ○ 5.2.9.4 - Mean time between failures (MTBF)	
5.3	Explain the processes associated with third-party risk assessment and management 5.3.1 - Vendor assessment ○ 5.3.1.1 - Penetration testing ○ 5.3.1.2 - Right-to-audit clause ○ 5.3.1.3 - Evidence of internal audits ○ 5.3.1.4 - Independent assessments ○ 5.3.1.5 - Supply chain analysis 5.3.2 - Vendor selection ○ 5.3.2.1 - Due diligence ○ 5.3.2.2 - Conflict of interest 5.3.3 - Agreement types ○ 5.3.3.1 - Service-level agreement (SLA) ○ 5.3.3.2 - Memorandum of agreement (MOA) ○ 5.3.3.3 - Memorandum of understanding (MOU) ○ 5.3.3.4 - Master service agreement (MSA) ○ 5.3.3.5 - Work order (WO)/statement of work (SOW) ○ 5.3.3.6 - Non-disclosure agreement (NDA) ○ 5.3.3.7 - Business partners agreement (BPA) 5.3.4 - Vendor monitoring 5.3.5 - Questionnaires 5.3.6 - Rules of engagement	7.4 9.4 10.4 12.2 13.2
5.4	Summarize elements of effective security compliance 5.4.1 - Compliance reporting ○ 5.4.1.1 - Internal ○ 5.4.1.2 - External	6.2 13.1, 13.2

	5.4.2 - Consequences of non-compliance ○ 5.4.2.1 - Fines ○ 5.4.2.2 - Sanctions ○ 5.4.2.3 - Reputational damage ○ 5.4.2.4 - Loss of license ○ 5.4.2.5 - Contractual impacts 5.4.3 - Compliance monitoring ○ 5.4.3.1 - Due diligence/care ○ 5.4.3.2 - Attestation and acknowledgement ○ 5.4.3.3 - Internal and external ○ 5.4.3.4 - Automation 5.4.4 - Privacy ○ 5.4.4.1 - Legal implications ○ 5.4.4.1.1 - Local/regional ○ 5.4.4.1.2 - National ○ 5.4.4.1.3 - Global ○ 5.4.4.2 - Data subject ○ 5.4.4.3 - Controller vs. processor ○ 5.4.4.4 - Ownership ○ 5.4.4.5 - Data inventory and retention ○ 5.4.4.6 - Right to be forgotten	
5.5	Explain types and purposes of audits and assessments 5.5.1 - Attestation 5.5.2 - Internal ○ 5.5.2.1 - Compliance ○ 5.5.2.2 - Audit committee ○ 5.5.2.3 - Self-assessments 5.5.3 - External ○ 5.5.3.1 - Regulatory ○ 5.5.3.2 - Examinations ○ 5.5.3.3 - Assessment ○ 5.5.3.4 - Independent third-party audit 5.5.4 - Penetration testing ○ 5.5.4.1 - Physical ○ 5.5.4.2 - Offensive ○ 5.5.4.3 - Defensive	6.2, 6.5 7.4 12.3

	○ 5.5.4.4 - Integrated ○ 5.5.4.5 - Known environment ○ 5.5.4.6 - Partially known environment ○ 5.5.4.7 - Unknown environment ○ 5.5.4.8 - Reconnaissance ○ 5.5.4.8.1 - Passive ○ 5.5.4.8.2 - Active	
5.6	Given a scenario, implement security awareness practices 5.6.1 - Phishing ○ 5.6.1.1 - Campaigns ○ 5.6.1.2 - Recognizing a phishing attempt ○ 5.6.1.3 - Responding to reported suspicious messages 5.6.2 - Anomalous behavior recognition ○ 5.6.2.1 - Risky ○ 5.6.2.2 - Unexpected ○ 5.6.2.3 - Unintentional 5.6.3 - User guidance and training ○ 5.6.3.1 - Policy/handbooks ○ 5.6.3.2 - Situational awareness ○ 5.6.3.3 - Insider threat ○ 5.6.3.4 - Password management ○ 5.6.3.5 - Removable media and cables ○ 5.6.3.6 - Social engineering ○ 5.6.3.7 - Operational security ○ 5.6.3.8 - Hybrid/remote work environments 5.6.4 - Reporting and monitoring ○ 5.6.4.1 - Initial ○ 5.6.4.2 - Recurring 5.6.5 - Development 5.6.6 - Execution	2.2 6.3, 6.6 7.3 10.9 13.2

Objective Mapping: LabSim Section to TestOut Security Pro Objective

Section	Title	Objectives
1.0	**Security Concepts**	
1.1	Security Introduction	
1.2	Security Controls	
1.3	Use the Simulator	
2.0	**Threats, Vulnerabilities, and Mitigations**	
2.1	Understanding Attacks	
2.2	Social Engineering	5.2 Assessment techniques • 5.2.2 Identify social engineering
2.3	Malware	3.1 Harden computer systems • 3.1.2 Configure anti-virus protection
3.0	**Cryptographic Solutions**	
3.1	Cryptography	4.2 Implement Encryption Technologies • 4.2.1 Encrypt data communications
3.2	Cryptography Implementations	4.2 Implement Encryption Technologies

		• 4.2.1 Encrypt data communications • 4.2.2 Encrypt files
3.3	Hashing	4.2 Implement Encryption Technologies • 4.2.1 Encrypt data communications
3.4	Encryption	4.2 Implement Encryption Technologies • 4.2.2 Encrypt files
3.5	Public Key Infrastructure	4.2 Implement Encryption Technologies • 4.2.3 Manage certificates
4.0	**Identity and Access Management**	
4.1	Access Control Models	
4.2	Authentication	
4.3	Authorization	
4.4	Active Directory Overview	1.1 Manage identity • 1.1.1 Manage Windows local and domain users and groups • 1.1.3 Manage Active Directory OUs 1.2 Harden authentication • 1.2.5 Configure and link Group Policy Objects (GPO)

4.5	Hardening Authentication	1.2 Harden authentication • 1.2.1 Configure account policies • 1.2.2 Manage account password • 1.2.3 Secure default and local accounts • 1.2.4 Enforce User Account Control (UAC) • 1.2.5 Configure and link Group Policy Objects (GPO)
4.6	Linux Users	1.1 Manage identity • 1.1.2 Manage Linux users and groups 1.2 Harden authentication • 1.2.2 Manage account password • 1.2.3 Secure default and local accounts
4.7	Linux Groups	1.1 Manage identity • 1.1.2 Manage Linux users and groups
4.8	Remote Access	2.2 Harden network devices • 2.2.3 Configure and access a Virtual Private Network (VPN)
4.9	Network Authentication	
5.0	**Network Architecture**	

5.1	Enterprise Network Architecture	
5.2	Security Appliances	2.1 Harden physical access • 2.1.2 Install and configure a security appliance • 2.1.4 Create and configure a screened subnet
5.3	Screened Subnets	2.1 Harden physical access • 2.1.4 Create and configure a screened subnet
5.4	Firewalls	2.1 Harden physical access • 2.1.3 Install and configure a firewall
5.5	Virtual Private Networks	2.2 Harden network devices • 2.2.3 Configure and access a Virtual Private Network (VPN) • 2.2.4 Harden a wireless network
5.6	Network Access Control	
5.7	Network Device Vulnerabilities	2.2 Harden network devices • 2.2.1 Configure and access a switch
5.8	Network Applications	
5.9	Switch Security and Attacks	2.2 Harden network devices • 2.2.1 Configure and access a switch

5.10	Router Security	2.2 Harden network devices • 2.2.5 Configure router security
6.0	**Resiliency and Site Security**	
6.1	Physical Threats	2.1 Harden physical access • 2.1.1 Implement physical security
6.2	Monitoring and Reconnaissance	2.2 Harden network devices • 2.2.4 Harden a wireless network
6.3	Intrusion Detection	5.2 Assessment techniques • 5.2.1 Implement intrusion detection
6.4	Protocol Analyzers	
6.5	Analyzing Network Attacks	5.2 Assessment techniques • 5.2.4 Analyze network attacks • 5.2.5 Analyze password attacks
6.6	Analyzing Password Attacks	5.2 Assessment techniques • 5.2.2 Identify social engineering • 5.2.5 Analyze password attacks
7.0	**Vulnerability Management**	

7.1	Vulnerability Management	3.1 Harden computer systems • 3.1.4 Configure Windows Update 5.2 Assessment techniques • 5.2.3 Scan for vulnerabilities
7.2	Vulnerability Scanning	5.2 Assessment techniques • 5.2.3 Scan for vulnerabilities
7.3	Alerting and Monitoring	3.1 Harden computer systems • 3.1.2 Configure anti-virus protection 4.2 Implement Encryption Technologies • 4.2.1 Encrypt data communications • 4.2.2 Encrypt files 5.1 Implement logging and auditing • 5.1.2 Enable device logs
7.4	Penetration Testing	5.2 Assessment techniques • 5.2.3 Scan for vulnerabilities
8.0	**Network and Endpoint Security**	
8.1	Operating System Hardening	1.1 Manage identity

		• 1.1.1 Manage Windows local and domain users and groups 1.2 Harden authentication • 1.2.5 Configure and link Group Policy Objects (GPO) 2.1 Harden physical access • 2.1.3 Install and configure a firewall 3.1 Harden computer systems • 3.1.2 Configure anti-virus protection • 3.1.4 Configure Windows Update 3.2 Implement application defenses • 3.2.1 Implement an application allow list
8.2	File Server Security	3.1 Harden computer systems • 3.1.1 Configure file system inheritance • 3.1.3 Configure NTFS permissions 4.2 Implement Encryption Technologies • 4.2.2 Encrypt files
8.3	Linux Host Security	2.1 Harden physical access • 2.1.3 Install and configure a firewall

8.4	Wireless Overview	2.2 Harden network devices • 2.2.2 Configure and access a wireless network
8.5	Wireless Attacks	2.2 Harden network devices • 2.2.2 Configure and access a wireless network • 2.2.4 Harden a wireless network
8.6	Wireless Defenses	2.2 Harden network devices • 2.2.2 Configure and access a wireless network • 2.2.4 Harden a wireless network
8.7	Data Transmission Security	3.2 Implement application defenses • 3.2.3 Configure web application security 4.2 Implement Encryption Technologies • 4.2.1 Encrypt data communications
8.8	Web Application Security	3.2 Implement application defenses • 3.2.3 Configure web application security • 3.2.5 Configure browser settings
8.9	Application Development and Security	3.2 Implement application defenses • 3.2.1 Implement an application allow list

		• 3.2.2 Implement Data Execution Prevention (DEP)
9.0	**Incident Response**	
9.1	Incident Response and Mitigation	5.2 Assessment techniques • 5.2.4 Analyze network attacks • 5.2.5 Analyze password attacks
9.2	Log Management	5.1 Implement logging and auditing • 5.1.2 Enable device logs 5.2 Assessment techniques • 5.2.1 Implement intrusion detection • 5.2.3 Scan for vulnerabilities
9.3	Digital Forensics	
9.4	Redundancy	4.1 Protect and Maintain Data files • 4.1.2 Implement redundancy
9.5	Backup and Restore	4.1 Protect and Maintain Data files • 4.1.1 Perform data backups and recovery
10.0	**Protocol, App, and Cloud Security**	

10.1	Host Virtualization	3.3 Implement virtualization • 3.3.1 Create virtual machines • 3.3.2 Create virtual switches 5.2 Assessment techniques • 5.2.3 Scan for vulnerabilities
10.2	Virtual Networking	3.3 Implement virtualization • 3.3.1 Create virtual machines • 3.3.2 Create virtual switches
10.3	Software-Defined Networking	
10.4	Cloud Services	
10.5	Mobile Devices	2.2 Harden network devices • 2.2.6 Bring Your Own Device (BYOD) security
10.6	Mobile Device Management	2.2 Harden network devices • 2.2.6 Bring Your Own Device (BYOD) security 3.2 Implement application defenses • 3.2.1 Implement an application allow list
10.7	BYOD Security	2.2 Harden network devices

		• 2.2.2 Configure and access a wireless network • 2.2.6 Bring Your Own Device (BYOD) security
10.8	Embedded and Specialized Systems	
10.9	Email	3.2 Implement application defenses • 3.2.1 Implement an application allow list • 3.2.4 Configure email filters and settings • 3.2.5 Configure browser settings
11.0	**Security Governance Concepts**	
11.1	Policies, Standards, and Procedures	
11.2	Change Management	
11.3	Automation and Orchestration	
12.0	**Risk Management Processes**	
12.1	Risk Management Processes and Concepts	
12.2	Vendor Management	
12.3	Audits and Assessments	1.2 Harden authentication • 1.2.5 Configure and link Group Policy Objects (GPO)

		5.1 Implement logging and auditing • 5.1.1 Configure advanced audit policy • 5.1.2 Enable device logs
13.0	**Data Protection and Compliance**	
13.1	Data Classification and Compliance	
13.2	Personnel Policies	
A.0	**CompTIA Security+ SY0-701 - Practice Exams**	
A.1	Prepare for CompTIA Security+ SY0-701 Certification	
A.2	CompTIA Security+ Domain Review (20 Questions)	
A.3	CompTIA Security+ Domain Review (All Questions)	
B.0	**TestOut Security Pro - Practice Exams**	
B.1	Prepare for TestOut Security Pro Certification	
B.2	TestOut Security Pro Domain Review	

Objective Mapping: TestOut Security Pro Objective to LabSim Section

#	Domain	Module.Section
1.0	**Identity Management and Authentication**	
1.1	Manage identity 1.1.1 Manage Windows local and domain users and groups 1.1.2 Manage Linux users and groups 1.1.3 Manage Active Directory OUs	4.4, 4.6, 4.7 8.1
1.2	Harden authentication 1.2.1 Configure account policies 1.2.2 Manage account password 1.2.3 Secure default and local accounts 1.2.4 Enforce User Account Control (UAC) 1.2.5 Configure and link Group Policy Objects (GPO)	4.4, 4.5, 4.6 8.1 12.3
2.0	**Physical and Network Security**	
2.1	Harden physical access 2.1.1 Implement physical security 2.1.2 Install and configure a security appliance 2.1.3 Install and configure a firewall 2.1.4 Create and configure a screened subnet 2.1.5 Configure Network Address Translation (NAT)	5.2, 5.3, 5.4 6.1 8.1, 8.3
2.2	Harden network devices 2.2.1 Configure and access a switch 2.2.2 Configure and access a wireless network	4.8 5.5, 5.7, 5.9, 5.10

	2.2.3 Configure and access a Virtual Private Network (VPN) 2.2.4 Harden a wireless network 2.2.5 Configure router security 2.2.6 Bring Your Own Device (BYOD) security 2.2.7 Create and connect to a Virtual Local Area Network (VLAN)	6.2 8.4, 8.5, 8.6 10.5, 10.6, 10.7
3.0	**Host and Application Defense**	
3.1	Harden computer systems 3.1.1 Configure file system inheritance 3.1.2 Configure anti-virus protection 3.1.3 Configure NTFS permissions 3.1.4 Configure Windows Update	2.3 7.1, 7.3 8.1, 8.2
3.2	Implement application defenses 3.2.1 Implement an application allow list 3.2.2 Implement Data Execution Prevention (DEP) 3.2.3 Configure web application security 3.2.4 Configure email filters and settings 3.2.5 Configure browser settings	8.1, 8.7, 8.8, 8.9 10.6, 10.9
3.3	Implement virtualization 3.3.1 Create virtual machines 3.3.2 Create virtual switches	10.1, 10.2
4.0	**Data Security**	
4.1	Protect and Maintain Data files 4.1.1 Perform data backups and recovery	9.4, 9.5

	4.1.2 Implement redundancy	
4.2	Implement Encryption Technologies 4.2.1 Encrypt data communications 4.2.2 Encrypt files 4.2.3 Manage certificates	3.1, 3.2, 3.3, 3.4, 3.5 7.3 8.2, 8.7
5.0	**Audit and Security Assessment**	
5.1	Implement logging and auditing 5.1.1 Configure advanced audit policy 5.1.2 Enable device logs	7.3 9.2 12.3
5.2	Assessment techniques 5.2.1 Implement intrusion detection 5.2.2 Identify social engineering 5.2.3 Scan for vulnerabilities 5.2.4 Analyze network attacks 5.2.5 Analyze password attacks	2.2 6.3, 6.5, 6.6 7.1, 7.2, 7.4 9.1, 9.2 10.1